The Sin Digoo Affair

- **URL:**http://www.secureworks.com/research/threats/sindigoo/
- **Date:** 29 February 2012
- **Author:** Joe Stewart, *Director of Malware Research*, Dell SecureWorks Counter Threat Unit Research Team

"We cannot enter into informed alliances until we are acquainted with the designs of our neighbors and the plans of our adversaries." - Sun Tzu, The Art of War

Introduction

The story of the Sin Digoo affair begins with a set of Internet domain registrations dating back to 2004. Between 2004 and 2011, a person using the email address jeno_1980@hotmail.com registered several domains using the names "Tawnya Grilth" and "Eric Charles". Curiously, all of the "Tawnya Grilth" domains showed the registrant's physical address to be a post office box in the fictional/misspelled town of "Sin Digoo", California.

Figure 1. Characteristics of domains registered by jeno_1980@hotmail.com.

In 2006 and 2007, jeno_1980@hotmail.com registered a number of domains under the "Tawnya Grilth" alias that have appeared repeatedly on reports published by various automated malware analysis systems and antivirus websites. The Dell SecureWorks CTU[SM] research team examined malware samples using these domains and concluded that these domains were involved in a larger pattern of malware-based espionage, sometimes referred to as Advanced Persistent Threat (APT) activity.

Espionage malware

There are two primary malware families involved with the Sin Digoo domains. One is known as "Enfal", which is short for "EtenFalcon", a string found inside early samples. The involvement of actors using this malware for espionage was first detailed in 2010 in a joint report by the Information Warfare Monitor and the Shadowserver Foundation. The report, titled "Shadows in the Cloud: Investigating Cyber Espionage 2.0," was a continuation of research from an earlier report titled "Tracking GhostNet: Investigating a Cyber Espionage Network." A later report by antivirus firm Trend Micro titled "The LURID Downloader" further details a campaign of espionage by this malware against targets worldwide.

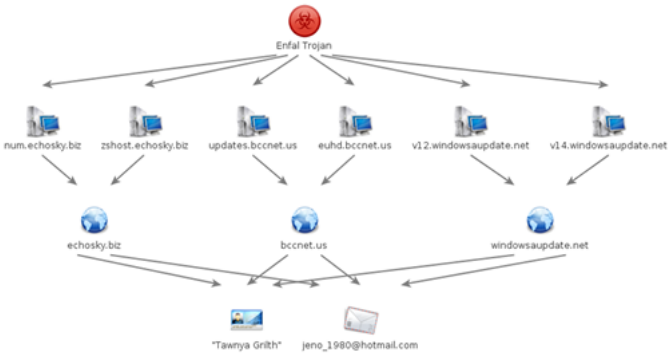

Figure 2. Sin Digoo connection to Enfal malware.

A second family of malware connecting to the "Tawnya Grilth" domains is less well-known, although a couple of antivirus companies have used the names "RegSubsDat", "RegSubDat" or "Kirpich" to refer to it. A recent variant was described by the information security firm CyberESI in a 2011 blog post titled "India-United States Naval Cooperation.doc Analysis." Details regarding the earlier variant used in the Sin Digoo activity was first analyzed in a blog posting by Don C. Weber titled "Malware Characteristics Report - Trojan.RegSubsDat.A" on his Security Ripcord blog.

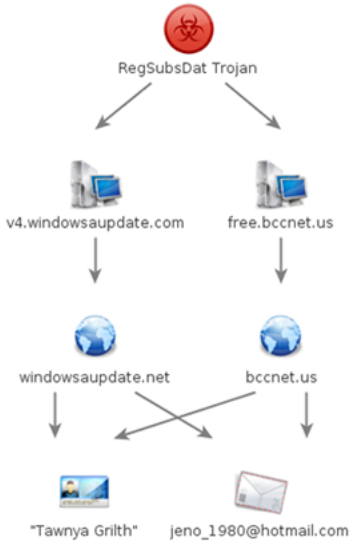

Figure 3. Sin Digoo connection to RegSubsDat malware

Although windowsaupdate.com is not a "Tawnya Grilth" domain according to the WHOIS data, the name is almost certainly related to the domain windowsaupdate.net, especially given the same subdomain naming pattern (e.g., v4, v12, v14).

Victim discovery

CTU analysts sinkholed a number of the "Tawnya Grilth" domains in 2011 and 2012. Traffic from infected victim computers is now sent to servers that log connections, gather statistics, and notify victims when possible. The initial findings from the sinkholing activity are:

1. Between 100 and 200 computers located in Vietnam, Brunei, and Myanmar are infected by RegSubsDat. Analysis of the IP addresses connecting to the sinkhole show that many are government ministries. Additionally, more than one regional petroleum company and a newspaper has been infected.
2. A handful of victim computers in Europe and the Middle East are infected by RegSubsDat, Enfal, and one other unknown trojan. These computers belong to government ministries in different countries, an embassy, a nuclear safety agency, and other business-related groups. Additionally, there is an embassy located inside mainland China that is infected.

The CTU researchers have notified many of the national computer security incident response teams (CSIRTs) in the countries where infections were detected and are continuing this notification process. The notifications include the necessary information to locate victims within the country, inform the victims, and mitigate the infections.

Link to RSA breach

In addition to the GhostNet link, connections can also be drawn between the malware used in the Sin Digoo activity and the RSA breach revealed in early 2011. According to the US-CERT EWIN-11-077 bulletin, a number of command-and-control (C2) hostnames used by RegSubsDat shared three different IP addresses at different points in time, with one of the hostnames known to be part of the RSA breach. This C2 hostname was used in a piece of malware known as "Murcy", which was detailed in "Command and Control in the Fifth Domain," a 2012 report by Command Five Pty Ltd.

Figure 4. Connection between the RegSubsDat malware and the Murcy malware.

All three IP addresses belong to the China Beijing Province Network (AS4808). Although the RegSubsDat and Murcy C2s shared these IPs a few months apart, the fact that three IP different addresses at the same ISP overlapped in a short time frame seems to indicate shared infrastructure used by both the RSA breach actors and other actors using the RegSubsDat malware. AS4808 is known for many other connections to malware and is considered by some to be a hotbed of espionage C2s, especially the 123.120.96.0/19, 114.248.80.0/20 and 114.248.96.0/20 subnets. These subnets have been seen in DNS records for hundreds of C2 hostnames for dozens of custom malware families, either known for or

suspected in espionage activity.

The RegSubsDat asia-online.us domain was registered by an unknown actor using the email address king_public@hotmail.com. A 2011 blog posting by "Cyb3rsleuth" traced this email address to a social media profile created by a person living in Beijing named "Wang Liang Chen." The same email address was used to register many other RegSubsDat domains as well. The social media profile for king_public@hotmail.com has since been deleted.

Tracking Tawnya

The same type of open-source intelligence can be used to gather information about the jeno_1980@hotmail.com actor. One domain registered by jeno_1980@hotmail.com is "socialup.net". This site describes a "like exchange," which is a service that Internet marketers can use to promote a story on social media sites like Digg or Reddit.

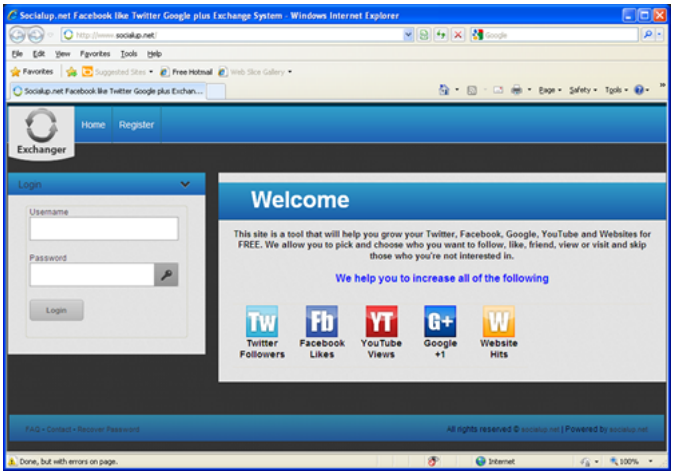

Figure 5. Screenshot of the socialup.net interface.

This type of service falls under the category of "blackhat SEO," a term for a variety of techniques for manipulating search engines and social media sites for marketing purposes. These methods are considered "blackhat" because they usually lead to a site or user being banned from the search engine or social media sites if the manipulation is discovered.

The socialup.net website has been repeatedly promoted on blackhat SEO message boards by various personas, including one named "Tawnya".

Figure 6. Example of "Tawnya" promoting socialup.net.

Once a user signs up with socialup.net, they can earn virtual "coins." The coins can be used to promote the user's websites or social media posts, either by viewing ads or liking other users' stories and links. A user can also buy coins from the owner of socialup.net using PayPal.

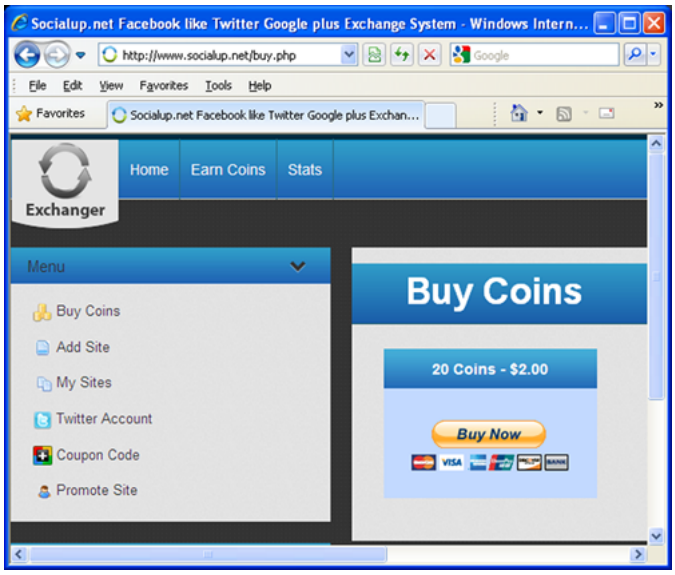

Figure 7. Example of interface to purchase coins.

As part of the PayPal transaction, the potential customer can see the payee email address. In the case of socialup.net, PayPal's website shows that the payment for the socialup.net coins is sent to an individual with the initials jzd.

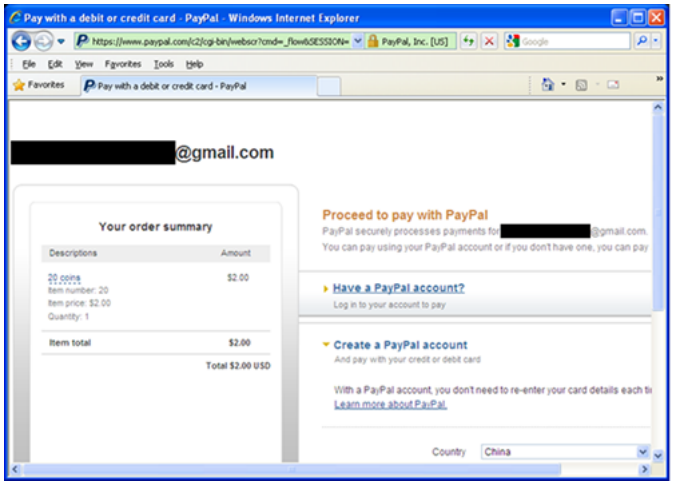

Figure 8. Order summary for coins showing payee information.

One of the other "Tawnya Grilth" domains is "i-tobuy.com". This domain was registered in 2004 using the jeno_1980@hotmail.com email address and "Sin Digoo" location, but the nickname "xxgchappy" is also shown in the registrant contact data.

```
Registration Service Provided By: Jarphon Domain
Contact: admin@jarphon.com
Visit:

Domain name: i-tobuy.com

Registrant Contact:
    xxgchappy
    tawnya grilth (jeno_1980@hotmail.com)
    +1.3155235526
    Fax: +1.3155235526
    po box 103
    sin digoo, CA RG7 8NN
    US
```

Figure 9. Registrant contact data for i-tobuy.com.

Another domain registered in 2004 using the "Sin Digoo" location was "1stsale.net", registered to a "john twk" with the email address xxgchappy@vip.sina.com.

```
Registration Service Provided By: NameCheap.com
Contact: support@NameCheap.com
Visit: http://www.namecheap.com/

Domain name: 1stsale.net

Registrant Contact:
    ak meida
    john twk (xxgchappy@vip.sina.com)
    +1.8213313311
    Fax: none
    po box 213
    sin digoo, ca 92451
    US
```

Figure 10. Registrant contact data for 1stsale.net.

There is a profile on a Chinese programmers' forum for an "xxgchappy" user who has posted two different email addresses in different messages on the site. These addresses are xxgchappy@vip.sina.com and [redacted]@sina.com.cn (address redacted). The user's name is listed on the forum's profile page for "xxgchappy" and contains the initials ZD.

Figure 11. Profile for xxgchappy.

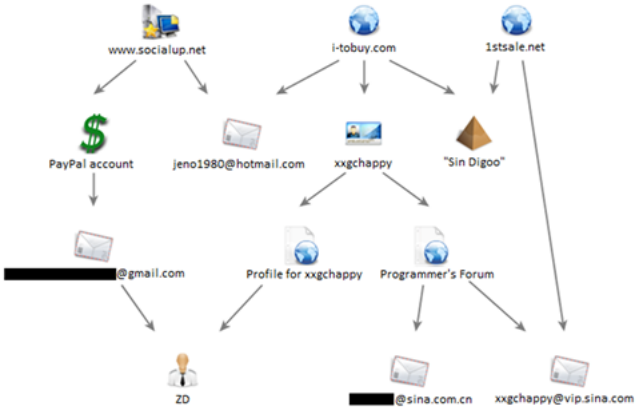

Figure 12. Tracing the connections between socialup.net, i-tobuy.com, and 1stsale.net.

Several clues on the Internet point to xxgchappy, or ZD, having a working knowledge of computer programming. The use of the programmers' forum, along with postings to that site, indicates he is interested in code related to hooking Windows API functions, a common technique used in malware. Additionally, both xxgchappy@vip.sina.com and king_public@hotmail.com were the listed email addresses for users of the "rootkit.com" site, revealed when that site's database was leaked in 2011.

A "rootkit" is a program used for hiding traces of malware on a system, and rootkit.com was a forum for discussing the latest rootkit technolo-

gies. However, simply having an account on rootkit.com does not imply one is using rootkits offensively — many anti-malware researchers were also members of the site. There are some interesting clues in the database table for both users.

The nickname "Jeno" appears again in the rookit.com user database entry for the user with the email address xxgchappy@vip.sina.com.

(7523,'Jeno','91cec994','Jeno Alix','xxgchappy@vip.sina.com',1,0,
'','','','','',0,'http://www.rootkit.com/usericons/Jeno.jpg',''
,1265784473,'123.6.89.98',0,0,0,1265721022,0,0,0,'','0','','',-1,''),

(23025,'king-rose','e211f11c0b28434bf7f1c8fb510fa9ae','Club-tom',
'king_public@hotmail.com',1,1106582903,'','','','','',0,''
,1106837367,'61.51.59.63',0,0,0,1106583113,0,0,0,'BH','19800126',
'','',0,''),

Figure 13. Database entries with the xxgchappy and king_public email addresses.

In the entry for king_public@hotmail.com, we see the nicknames "king-rose" and "Club-tom", but even more interesting is the password hash "e211f11c0b28434bf7f1c8fb510fa9ae". This password hash appears in only one other entry in the rootkit.com database:

(20446,'king-z','e211f11c0b28434bf7f1c8fb510fa9ae','k,z,y',
'wzy_100@hotmail.com',1,1097652186,'','','','','',0,'','',1284013010,
'123.120.127.153',0,0,0,1284013010,0,0,0,'','','','','',0,''),

Figure 14. Other appearance of the password hash associated with king_public@hotmail.com.

From this evidence, we can deduce that "king-z" is a second, earlier account of king_public@hotmail.com, created using the wzy_100@hotmail.com email address. Even more interesting is the 123.120.127.153 IP address the king-z account used to log in. This IP is located inside one of the AS4808 netblocks famous for espionage activity. In fact, it is remarkably close to 123.120.127.159, an IP used by Enfal C2 v2.windowsaupdate.net (one of the "Tawnya Grilth" domains) on September 27, 2010. The last account activity for king-z as shown in the rootkit.com database is September 9, 2010. This data strongly suggests that king_public@hotmail.com is not just a stolen account used to register a domain, but that the user is involved in the espionage network in some manner.

The password used by xxgchappy@vip.sina.com does not appear elsewhere in the leaked rootkit.com database; however, another leaked database may provide additional clues surrounding the xxgchappy personality.

The @sina.com.cn (address redacted) email address associated with the user xxgchappy can be found inside an archive posted to the "hackchina.com" website.

xxgchappy # 2710 # @sina.com.cn

Figure 15. xxgchappy reference from the hackchina.com website.

The archive contains a denial-of-service attack tool called "lankiller". Inside the lankiller binary is the following comment:

Designed for lyh by xxgc-happy 2002.3.8

Figure 16. Reference to xxgc-happy in the lankiller tool.

Also included in the lankiller archive is a README file that describes the use of the tool. It asks the user to email the author at either @sina.com.cn or happy@sohu.com.cn.

Figure 17. Email addresses referenced in the lankiller README file.

There is a profile for "happy" on a Chinese video site showing a possible photo of the user. The photo is of a man who appears to be in his early twenties and of Asian descent.

Conclusion

The Sin Digoo activity is only a limited view into a very large amount of espionage-by-malware that is happening in the world. The Enfal, RegSubsDat, and Murcy malware families possess dozens of defunct and active C2s, and these three trojans are only a tiny subset of the malware families the Dell SecureWorks CTU research team knows to be involved in espionage activity. Collaboration between government, espionage malware victims, and the computer security industry must improve to better defend against this undercurrent of activity that threatens to undermine an already weakened economy in countries around the world.

Appendix A – Network IDS signatures

alert tcp $HOME_NET any -> any any (msg:"Enfal Trojan Activity"; flow:established,to_server; content:"GET|20|"; depth:4; pcre:"/^GET\x20.*\x2ftrandocs\x2fnetstate*\x20HTTP\x2f1/"; reference:url,www.secureworks.com/research/threats/sindigoo/; sid:1111111111;)

alert tcp $HOME_NET any -> any any (msg:"Enfal Trojan Activity"; flow:established,to_server; content:"GET|20|"; depth:4; pcre:"/^GET\x20.*\x2f(category2|data\x2fforum|httpdocs\x2fmm|trandocs\x2fmm).*[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]
{2}\x2f(showNumber|WindowTask|ORDERTIP|ComMand\x2esec|Cmwhite|ComMand\x2esec|Command.txt|Query.txt|sunrise|Tiblue|
reference:url,www.secureworks.com/research/threats/sindigoo/; sid:1111111112;)

alert tcp $HOME_NET any -> any any (msg:"Enfal Trojan Activity"; flow:established,to_server; content:"POST|20|"; depth:5; content:!"|0a|Referer|3a20|"; pcre:"/^POST\x20.*\x2fcg[a-z]\x2dbin\x2f(Clnpp5|CMS_ClearAll|CMS_ListImg|CMS_SubitAll|dieosn83|Dskx8|Htrc3|Info|Owpp4|Owpq4|Rwpq1|Trpq8|Trpq8|v
reference:url,www.secureworks.com/research/threats/sindigoo/; sid:1111111113;)

alert tcp $HOME_NET any -> any any (msg:"Enfal Trojan Activity"; flow:established,to_server; content:"POST|20|"; depth:5; pcre:"/^POST\x20.*\d{6,12}\x2ephp\x20HTTP\x2f1.*\r\n\r\n[a-z0-9\x2d]{4,15}\x3a[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]{2}\x2d[A-F0-9]{2}/s"; reference:url,www.secureworks.com/research/threats/sindigoo/; sid:1111111114;)

alert tcp $HOME_NET any -> any any (msg:"RegSubsDat Trojan Activity"; flow:established,to_server; content:"POST|20|"; depth:5; content:"|2f|log|20|HTTP|2f|1"; pcre:"/^POST\x20.*\x2f[A-F0-9]{6}0000\x2flog\x20HTTP\x2f1/"; reference:url,www.secureworks.com/research/threats/sindigoo/; sid:1111111115;)

Appendix B – Malware hashes

MD5 signatures for Enfal

0144f8d76662fc382b8eb094eb347e4b
01a5adace93ad5afac400f9589b62607
027d7db3d2a94bb0dfadc71300aaee3e
02857b2b6cc5aa750dbfb6a1088a5239
035f2e58144209ea9973bbe4cad58e15
04cb272bbe383707574005a2999f2fe0
054688eb39ea0cd380bb89b6746abc4f
06572d93d87a8d0fb7e070be79692c87
066be8f9e08acfe8ab1eecb884a73801
071d01bcaadc9df5683a6cfa81736714
084e99653956350210beb13c8ea43c79
09c44fcceb51f9affdb63b0d8f9e4b31
0a5446da47609868101c773e928b36e4
0bbd1f253e928cafa3c9c78cdaa849bd
0c589418274ba97663853d1c6bef3bd1
0ecd791525cc30ced610e81ef67290b0
0ed85a30083fb71452916e14a4b5936a
10162681b64c72834621c6fd68b6501f
106db67336a318b6ee4f3197027df85c
113a066b19737b59ab1e2ad921cf3a03
113bea934d89d0cfdc445489f0eb713d
11696e0f7399986c4978e35f3160c22b
1175fff7b282db3b2b0c8c9517bcd937
11cf5c71ddf9a666d9b470dff21c4ec5
13d82eaadf0a5f6fd2d76b66673efa91
140c69ea9a963100e75497b33820f1da
164e3c7488b70d6db28cf71cbc72b0c2
173ec685aa9f581a03c30866b5021574
17810c2ad162c4726729b3fc3ae8676e
184f2de39a9fcc0039eb9df09c4e75b8
19cddfee52c7b7adf4d5dd3e98e0b0bd
1c1f7b32d5381335b83af545b9eef101
1c2aab24d699c24cec860e73c767bce7
1e95875e6c0f054b62c94d6063ff9eed
1f91d940c42f216cf95e724a034802db
1fa520329a77d01aaaf5808ddf529ce2
21b761b4401d290b9e02fea87f2a9933
2370a2142bc61c520226d188e102a727
241aaa7d73339c1624a27fcce5d1815d
24decc7e98e67e3a6e5d34f284f79124
25710d277596d09e5607f419eb63e11d
272fffde11c97b31cf9de7c1e1816d61
276495490cf16318735f880785203378
2880436cf619a270e6c31d9da6eb426b
289242778ef037e02106a491de38cc1f
2944e486b252112720098860a91788e0
297158cfce8fc76789ca41899f6047ac
2ae27d10e04d229c937c0363c29ed3e8
2bc74b3aff2fd68eb38820bb0760f3a6
2bfd304e3433cb0de9c2f284e9417409
2f2f61d3b8f5064affb11e67ae6320b2
2fd6e2c7fc80ab9a6be6a0eebd09763e
2fdaa46fff13f87dcc22fb9aef9ba338
300dcc10df87a998b08dddd2dbc55a28
30971caaf134d7706c70335f54e3188f
30d075afef4e518f63c0b43b8c764e12
3270d18157131f216468cf7ce53ee8d1
331140c7ffaea93ed807f86720b5929e

331acc687cf2b93fc7bfed257ea54488
33eb9e349ec9e093c54028e7c1cd8b0a
340c9de8ff62134bb0e51c24c0919576
343cef9a8d83afca81918fc317f3ccb8
3447416fbbc65906bd0384d4c2ba479e
34563d4ccf2fdd8a08b05089d82a803b
347906343329916ace3636a541c96f26
34f53d0b59f7cf352aace044abf95df3
35369bf701904b17725429e8cb938645
35ca158ffd5965d68f7ef64ee527a028
3603c2b0262ed71402fe981991ddd614
367459c45eec216b6858e7b2f91e0c99
36b1f9def6a794ae0be8148d149e5fe7
36d10e8d5e95bcfed701df530de2a917
36dccde0de343af9e7f08128900334f2
36e8c4f5b906e2e4cc3d5e64b79b8642
374b6371918ab0ba91e9f3489e5eab19
39762af48276967a54372dca1f89936c
3b159b70f6f6e66db77dd6b57f04ec2f
3b5fdfff3f49f0231586dd4fcca7c25d
3c1c15ac3b1bf3787137685637e33140
3d176273201bb6f07746cd7c5c46166c
3d69e2b0257cebf9bc1a6f788f45fbcb
3e27d880674149d2548b5b36d22570ff
3fd66bcecc804913a016827eba28897a
427259dc60c10ca5586da8d76139cc92
42899a14835c5702af3c2f0abaf64429
4413e592ad3c072fa300f526b83bb644
442c0e4bda0035c34e767d429e7f821b
443ed084c7bb1687825670d0293d3482
453963093fa87f1ecd9be2691d080b0c
45b8270e80fcaa229cfe8e4baf15d9c2
45d07b1a0a6cea3035d448e384b59252
45f565e1b73e723ade1838e2c78867a6
46548ef50b1d64909f77a484bac66de6
46679d05a02e065a5f082d86d7635488
466cbf76ccf76e0a2fb309e9e8433bce
46a9e994658fe49e892c5a5d5740b58a
47bc44ccd673760918c99856a053aca0
48a4a92443dd2595806e9afd76275ea0
48ccdc7a5eec2a0240b28534d501eebb
4943c536c8b06044456af9971a0f54eb
499ad52953d3e12ebcda3f4eec3cad4f
49e0df6cb8abc6d4554829f2cc77ad75
4a828744a96d739815ff40d54bc9d022
4add8281a028c6ea76d369186f787004
4b835d7b89f754f72fa712fd281aa51f
4bb3264ddb68e096bbd11721fea3d2e2
4bc96cf2a63f4bfbc5f24c07329d986d
4cb5033c2b4e19872d2fb98dc9678362
4d84bd418da17f01298df489c251464f
4dc08c921bc81ce89aae397eaa049dda
4f862e38b7db5beebacff59a751b0f59
5098b3d6211a17f315fb33b17e37c9b1
50ecc77c6c831bcd7e0534353f61c479
514c992b5af684efb08ada784f36bce7
57ffbe0560b61ef7da39a29049dfdc45
5b0d5ad64256811a7e8be472f3492d2d

5b382d58d6a890ce696494c304242625
5c26947e42381afa8459b6a91308662e
5c2ebee0d8748e926d015d07c434b409
5c920ea7042f820f46ca8bdeb9a17519
5ccdc66a50b3b101d4038ab23b65196f
5cf7669f0b64b0780159cae4275e75e7
5dbd2ed78f47fd75112b5b8d9a5a2a7d
5f76d78402be896288284c18407957b2
5f84282c7ee466e777665ef72fa258b5
61792bb6aa26ce5e826ee300977825c1
61a605dc9bfcbdc382f528607115b8f1
629dc2675a940e6fd0cfd778f2c3149a
630e9ced15a16aaa464b73481297f40f
63d33065354038eec8b8a386d5bf45bf
6680e19b115c88416b13b5985bf2c32d
66fc71e3f35b3ef21cf524c3be92708c
67ae7ca090aed3841ca1c0ec85d26d2c
687cfc99f09f1cb9b1915135bc57fbbe
68a3e1c03a0ce92a648eea823bfcdd4d
690e6208ccfc960c71175e43c75deee1
6979c05ff1682c6bcff2da5f20350388
69f8825118ea8ab1c671c28298c592aa
6c1fa0a523a751b8d588b75814a46759
6e8994d01ab6837e6baeedbfd9bf45b2
701d95d5d716a726a4316d7352938510
70cf6edb22a2fd5fee7665ad1a260b39
70f167e43ba0c4df744601ace41d29fb
71313fcf3d825ba40375cf62f4777e10
719b1d9e93a6fe2fe0918f029990fbfd
72b9b505ef199fee23db350d6e096340
73802e2bb0c7f821f0959e9a424be35b
744670ca4531f7ceb72a75ae456e8215
74cb2fc990adf24f1da265dd14737d48
7547a4e39ac61eae20c79fa3834d8e2a
7578feae5abb684e691e44a1c82d0b78
7769907450c95de213567408d1c3eb32
79a160fec8c1e34b0188e034dffccfa5
7a1d4cba9ce2a28ef586c27689b5aea7
7a72460b0f3caeaa9a0dd5aa252a3dd5
7bd2cf1a96fe27c301111785799233ea
7c2258469a87138a94eb1a15578df9c1
7c9836391eb08e1cfa33dd1094d2f993
7db483b6dfb3952ce9c29b7bf26e662b
7e0d522932460ea1d9a88a82980b1234
7fd3760a10a79397da3e7f2531a3c165
7fec0946aa04ac5f96c8633565a503a7
80398a1c31cb0fad735d051f22865204
8042b3849217de1ee9181ee9c7338df8
80450d1256eddeece918ef02e9dedcd5
80a8635e966a5fb6924cfd92d18b1829
8198751a915561b30a607b1d2a651f73
81df7dca8b3bb3ae964fa8cfd82de413
81fa811f56247c236566d430ae4798eb
8279af9adb9dcde15f67e4938a32e460
83046fb020b98d6bdc59b6d3135fa293
8330e398c976797e86e23110255774ff
839ead900d516a2fe9ec7dc68c6f91dc
84356ed469c95c1418209bd929640622

84484706048822c4a483d9cdd4ae6136
845f298eeec87f92302146aba04ee108
84a201fa44c3675687ad2b9e3cf0adc1
84b8488ce8d20cab10fe10973429d1b3
84d24967cb5cbacf4052a3001692dd54
85639dd697e36a7eeb7e84e6ddccda46
856de08a947a40e00ea7ed66b8e02c53
858941e84af0d2a102b26497c22265c4
875b9628aee0a7108929ecd57f7e771d
89b61f9100b8135d7356fa864598be7f
89ffcc729bf4b89a298b0dd317228646
8bfc2763ec3141e6215fe9958607b895
8c6d058e3c821ca141cbbbcfe7afe8e8
8ec4fc310915b6db5d62ff476d95fc87
8fbc2220e1f505d3312542ccab2cb103
90506693e1df8190ad657d519551472d
908c8475c451050599909b0212857bbe
90bf1a608159df6c4f11f6366cecb998
912aad79475fd457165b3ae8c362203f
9133dcec65eb468ce226e1fd8accaf4e
923d3c72026a56bb9bc54843a6016854
925cbbd8060770e9175ce0433f03ad81
93cf1393241577797b36d707d4255faa
9604700eb71a14a540ba65429d2f75cd
97769f938619bf888a2750b4f079a134
9883cee2f281ae23c4929e0eba313876
9929a8ba088ec944b07c20e0d38d4355
996cdae702fe1f0b7555764c3f4daadd
99a0e8f84028813def520a9a7791635d
9a09e5acd4050a68ade420fcc79c6c66
9ab8cc0bd5facd7fed939ae8715c0f2f
9ac42be9c350de30415f73471b7ced64
9c909e8f3fdf46d1ab0246218f83dc71
9cc962a7f637aced6117aac78f74bdf5
9d001213c967234aef5207971b3dc084
9d0bc24173b98630f45f6cbb5aef048b
9dda46f5b3be826bf427ad6bbd8171ae
9fe79a8d9901cf773d272b0578c818c7
a03c312ad0309c02e29f3be32738f753
a1a977867a889be58767f3224806aef3
a25a0621c0381bdfe32b3f2ea6975f18
a4cc686615d113aa18e2f984a4d69dc6
a64e9189f49db0c1a1ae53891c8a69ef
a6d45978a7736e6265f0243bb14a4f1d
a6e2d6112100869191f20f49408c9459
a714c1df854f966161192b77ff2f4cd4
a78f479adda756ecea71246b6398ac4b
a83fc05a18e18ba19e93a75ffa6ebd50
a99fb261722f271234c872451512c67f
ab5d5a99c171d3e69490a9a7fbe3645f
ac1d99f4751ae8c28c452ae96d6bc800
ac7eccfce8dd486b830fe85dacaf35e8
ad7f7ce329139ccc252ed75704de2eab
ad92cbb5e3522fc4bfc15732284020d0
adab08e09dec4437be49a9346244375a
addd471dcbff1b125f993343a27819a7
ae4c9c1f16fbe20dd78da605f2091ad3
ae60f66d33259207e54ce03416c10adc

af5d3789bb5220553e7fc0d115be4655
b2c52b2078060c0d8dfe3f9c84ab0f1a
b60c862f6435247c21c7d2d05d804248
b9685cc3d0069135696fe51fd7258aac
ba2532bc122c881bfe4ddc39da1dfdf4
ba3324571e0f962e4d6aced7832f4d3f
bdfb76d4dd25ee3b4d36172a3c3cd98e
be7d72c4bb76831089176dd90188ad3e
bf0ad3625fd7cd2c8a7ba3fa74bf1605
bf35c5cb6763679914f267be25a54601
c0c04f41a823cdb4055b109dbadddd18
c1a8179ef14ae95d809179185bcc269f
c1ab14ce4612256bfc93c7b97e5f8353
c2b975caad371568904a04bbb9bf6e17
c3053ece751f9c0b2595a6d9350f48cf
c39183372160e75c7083a5c9eac68124
c3bac79122923eac3f1fd48c5775465d
c47fe9b7a3b72937adeb665432aeeff5
c4a6b6cf35ebed6d46eb5728a6247448
c524005b6f98f5428c228a9577e20f91
c576be490ae4b095149114b34c96c6a9
c5da1da605a6bfc4bf99721e6d665b8d
c6e5277717d0aa2ecd96e9ca06b195d1
c729c36ad0e32be7b23ad022ab8de27c
c7a7c668d4e5c80605bac305799d6ff2
c8a1c24bcd91ca21e89888e418153472
cd5ecadb214f3697d3c77e42c80aff71
d030c4df015cff67353065c0f7198058
d0b9b5889b3bc49ce4c4f942eef7e39f
d0d614ca7bf6745ad52910da8a672e1c
d1568b36e55fae5eb1b7a2ae3b9294f3
d1f641b6dd8861598af23557a7a52a3b
d414ce56e89e1db9df28c3dd388a8249
d415b7a5d328e32a0c383ce3889468af
d4baba6857f3682eeb8ae6f83cc9a271
d4f1188e75c55444a191649c4b4e1362
d541a9cca5288876676aae2ab962997f
d57379739354b204898149b456e732b3
d68d241572a8ffdc8a2e481c96baacfb
d837313adef94c3b173e0a9128896250
d84ecca01839642a27d29f885b885ff1
d8815fe64eb5321add412554908da28a
d8ca81ee8327d8314121d1560800674c
d8f21a32f7d33b1b6b5e948029410eb4
db3d36f3f8386f993a89c9bba25cbeaa
dd260e8a5462304621001dd3c12e4aa8
ddedcf6f543104a3485406d66068e263
dec5441851026a66a4ff0cfd008983c0
df87fe27fcda6906ae248663e0c62861
dfa055d94e59afa791b0f99ff82b54a6
e0417547ba54b58bb2c8f795bca0345c
e1833932053171da15c60e6c2fca708a
e21c8e1c3e79d669f13f771dbbe0eb77
e22632b517305aab6ba9691507d1d562
e31912492ef1edae863b34a96d8c529e
e38d44d1a226b9c1ca70a3e78beaf735
e3ead43315bcc851656805922309744f
e5d96aa540dd934aec72dcecafd366b8

e5ea0c7a48967202f25fc96d91a1a2cb
e61b128e97a39fe869cf89be571fe021
e691dc42a002e9f48f69cd33b70d8a15
e7f5a93eb76bab40d4aa088fba115aaf
e7f93c894451ef1fdefa81c6b229852c
e8664b135b6d681c812aa04ba14a120c
e875d971524d45c10cf332ebf7256688
eb0e2d5ebf6f3dbb4510b85c30a9751d
eb1dc493f005059c654817d153f7ee74
edbc569b5b5824a53721b71ad325a212
edfcb5ec135c94b77e4b94c2a82863b7
ee3ac02b6ca3d6c9012604d71017058f
eebfa7677dedd10edf4aca985f16284c
f03594793c06a097e4b1ac7e1d7079b8
f09e2e3a57d336cb65acab2bdd6b9d14
f1bb8a80e23b6c90004d97c7ef2d0454
f2627bf17528011130e5818bfac0afdb
f2a405326747245e5db97c60e878660b
f34195a2317bf079844bc44c92297cae
f36007400f0c85784fd374ad4ed23c6e
f362f47eb844f889bafd5a0e92c7cdf0
f3b95dad321a14500154e13cf3fbefe4
f3d302a8c56ea86d429157fde1793210
f50406b902601b005c1908a048489ca2
f50fa07be0222baffff05b23fdfd5b68
f5b65b971509eefa009d032003410faf
f77aff1d1c0d94cc96828fb88f3280f3
f7e3b90592c75a6c3c15336d34d97a9e
f9e64eba7185c266786857d7f933577b
fa3f412be4ebf45f478135221365dda7
fa7641771280db462f088d8353dbcfbd
fb11225f453365af4958f98bde2ce918
fc5364e8274a2eb8310d2528d78ac07e
fe4d6a3428cd9f87d5a7044d733d2299
ff271c14549b133a4475ad6615e894da

MD5 signatures for RegSubDat

01355596ec3596aa02b8c5f9f1adb5d6
030d492c8d12434144f9b1dc97928cb8
0434ae7b8267b08bd1c6ae17d6100353
048a3815cbf0b8dc9b4c3f680fcd913f
06054346974f309e1003faabac0d1dd5
0836b4a02971aaef33905a91799063ed
09e372c29e69e1edd29f02d4e660d33f
0cafb41eca73d768091bc93f4343cbb9
1050edb8cc0a073991bc637d590d89cc
12954f97e5db1cc86ecfe12be2ec7323
18f9d0973e60b13e7e28d0997e3a09e0
237d641b8267867b007ec94e0bbeff1a
2f6257eab8d3393ac6a96c490f1455ee
351f1ee0cc65d004d40183a7fb6ce616
36310e65b35780242d326f3f604b4c3f
3da70425c099ad4c050eaa4c3308d0cf

48c2d771e3083267a4f9e359ef0e53e5
49b7bc9ac3800caa49bca0a4b3350dbd
4ae7ac0060b938c50675ee2627e3c66d
52856c1a0c63509bf6c00ef1e9fca03c
58cde4ee026df987340a63cfc2c34318
5d53c97b800ca1519800b872bc3f9edf
5d88a3f713c610364fbf750f24af8257
646abf38720c7301698c32bec62d84ce
67d14ce17d3dab4a00d073b6315efc94
69f8d66ccd7fc63ee3f8a3e4f7d86f07
7019e8a17360a583931fb0908f31a2e2
7f7bf881da34242dd1927fda745812f1
81433a87eac3af2227623bf3239844de
83976d6937ebf841999f10bee38ab252
8b1c6478d620bfafbb2c5402d1f926c0
91c3ec270cca27a3785ac827a336c050
94d75acfc4c82c6e48e68b513ade057c
992fa71f3b5e4b1ca3a43d5b2a69e1c0
9a7f048e0e0d0f5bf117f19caef2db1f
9aa7d5ede53be461ab8c4d68fcaa50ab
9ec7da6881d2632a2e823176e915634b
9ef570a298116ac810fdde31a64c7631
a33ab32eeb02b677f9f2786dc3c0651c
a3a1ea2c99d40620fc8dee0222228f24
a876acf60d6e4c4da1123fc11f01ced7
aa90c8e524edb644286c5c0f6c5de987
af0aa267ced776b99a7d157294ac59ba
afd476bbc24a7f20afb017f6869fda65
b5b51dc06c3e9104fa59642952e69d49
b6352cc6e269277960a8da7c5f0306cd
c5860171f919761db9ee78ef3dac5ab4
c6a8c1cdeff0745427aafc588db9c59f
caf90ceece7242bb1147019daf14598f
cc683fc365ec57eea4bc8e1f80a66413
ce47cb6268087cf5c27d77259496989c
cff8e4eb16d010bcc33ad19eb807bd27
d408c2e627b3a895868bf16a3b228eac
dcb3b9ea717603bf6f42e7ce61ea3728
dd1e6b39afcba13b3df3eae13f26d888
e2aa3ca52b8ea17c4bb80d294fec8ec5
e78cc8790ff97eb13d448c15f3f3acae
ea20365eb2142afb4ab9a124808cb8c6
ecf15cce8bd4d6907d86ccff932b64af
ef80d287bd10af3b1cab06d01795ae1a
f5437d13428440412cbf5522adb25f8f
f9d2fec1684529f580785dda5820b372