Musical Chairs Playing Tetris

Sean Sabo (https://www.arbornetworks.com/blog/asert/author/ssabo/) on February 15, 2018. (https://www.arbornetworks.com/blog/asert/2018/02/)

February 20, 2018: This blog has been amended since it was originally published on February 15, 2018. This version removes the association with the APT group responsible for the Night Dragon campaign that we had incorrectly made. We thank the research team at Palo Alto Networks (https://www.paloaltonetworks.com/threat-research) for graciously bringing this to our attention.

Introduction

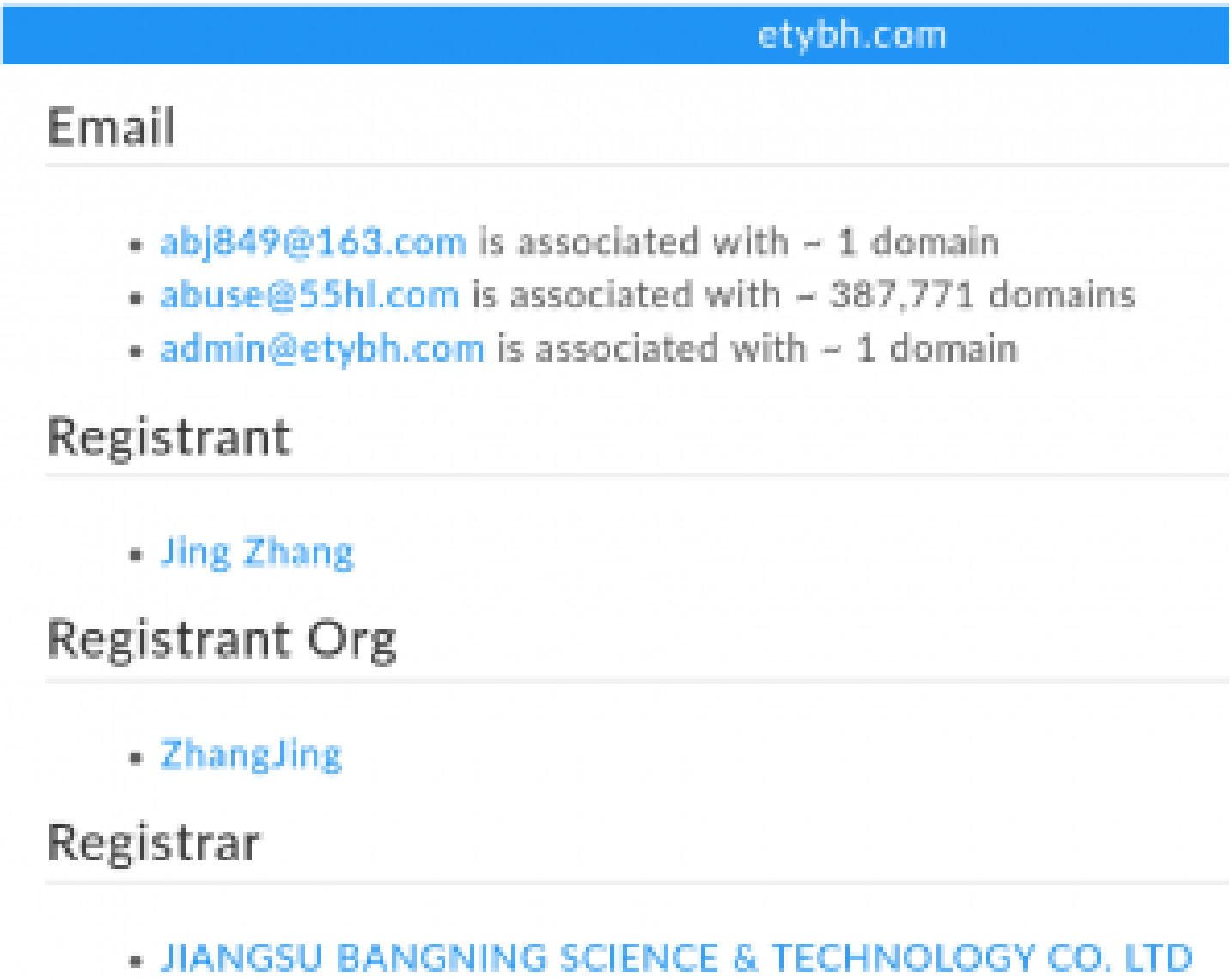
ASERT has discovered new command-and-control infrastructure controlled by the actors behind the Musical Chairs campaign. The actors are known for the longevity of their C2 domains, reusing them long after they have been identified, and for making use of a popular opened sourced RAT called Gh0st. Uniquely in our observation, they have even embedded a fully-functional version of the game Tetris that will launch only when a special condition is meet.

Key Findings

- ASERT has discovered a new domain associated with the actors behind the Musical Chairs campaign.
- This long-standing actor is known for maintaining static command-and-control infrastructure such as domains for long periods of time, even when they have been discovered and widely publicized in the community.
- With moderate confidence, ASERT expects this domain to be used in new intrusions.

Multiple (http://malware-unplugged.blogspot.com/2015/01/hunting-and-decrypting-communications.html) articles (https://www.sans.org/reading-room/whitepapers/detection/gh0st-dshell-decoding-undocumented-protocols-37032) have been written about Gh0st over the years, including this one discussing the Musical Chairs campaign (https://researchcenter.paloaltonetworks.com/2015/09/musical-chairs-multi-

year-campaign-involving-new-variant-of-gh0st-malware/)'s use of this RAT. **Using details from that report, ASERT has identified a new sample and more interestingly, a new domain that we have associated with the corresponding actor.**



(https://www.arbornetworks.com/blog/asert/wp-content/uploads/2018/02/domain_tools_etybh_com.png)

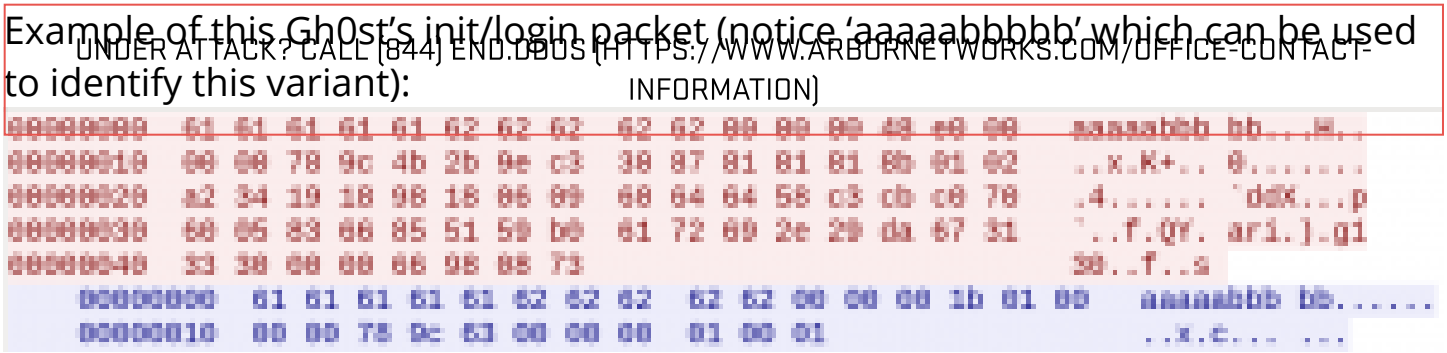
The sample appears to be delivered via an email according to artifacts provided by malware-traffic-analysis (http://www.malware-traffic-analysis.net/2018/01/04/index.html), which is consistent with documented tactics for this group (https://researchcenter.paloaltonetworks.com/2015/09/musical-chairs-multi-year-campaign-involving-new-variant-of-gh0st-malware/).

Gh0st variants are prolific as they can be found in a popular open-source source code repository – this blog provides the basis for our association with the actor.

Analysis

Malware

Example of this Gh0st's init/login packet (notice 'aaaaabbbbbb' which can be used to identify this variant):



(https://www.arbornetworks.com/blog/asert/wp-content/uploads/2018/02/gh0st_pcap.png)

Some other behavior of interest observed while reviewing this actor's specimen is they appear to be moving away from BAT and JS files as part of the infection process[i] to using DLL side loading. This is just one sample though, so take this for what it is. As part of the DLL side-loading, they make use of a signed executable to load a DLL which in turn is used to launch the actual Gh0st DLL. They are not the only malware authors who use this trick.

The observed functionality in this sample maps directly to public documentation for Gh0st, so this blog will not rehash that.

Association No. 1

Starting with the known C2 servers for this group, we can check to see if the new domain has any ties to them. Two of their C2s were registered back in 2013 and the campaign has been around even longer than that per

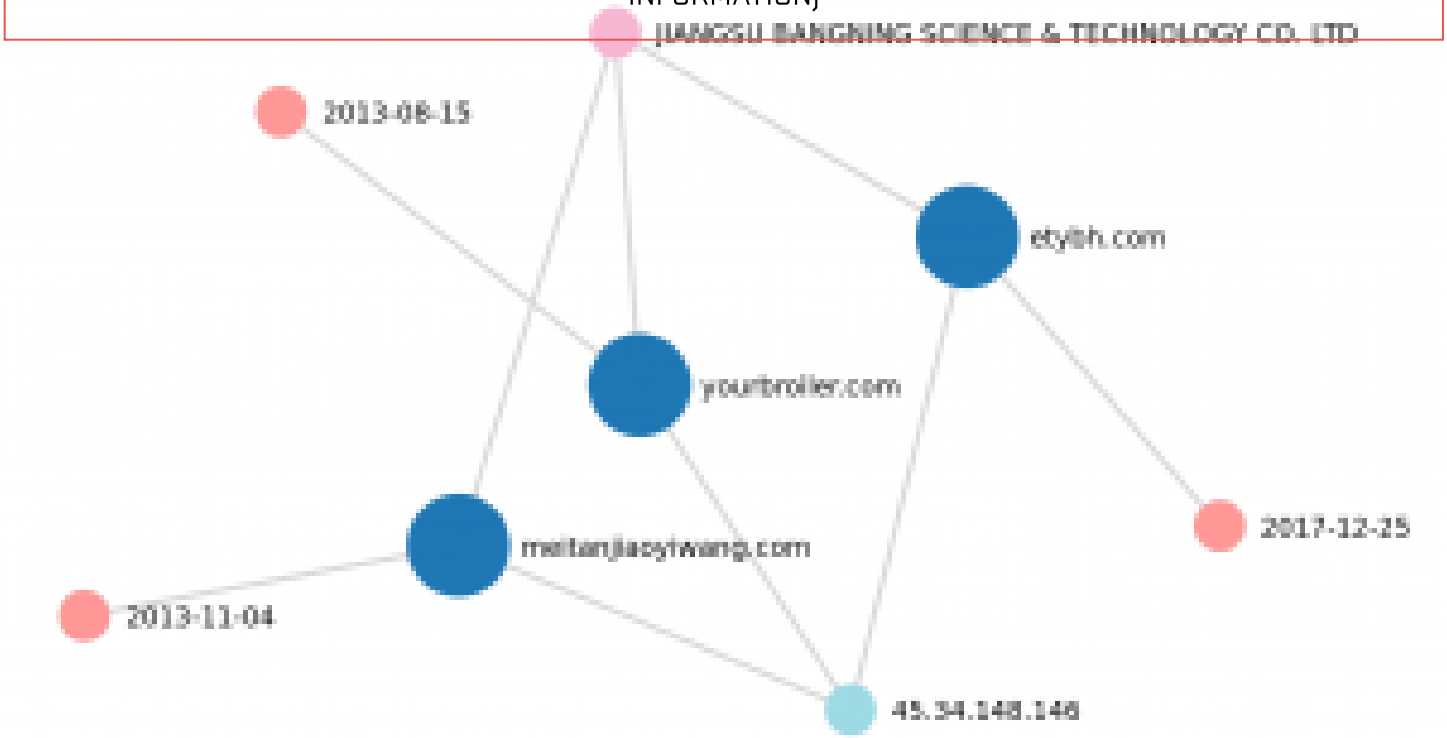
Known Domains

- yourbroiler[.]com
- meitanjiaoyiwang[.]com

New Domain

- etybh[.]com

Looking at DomainTools, we learn that all three share the same IP, 45.34.148.126, and the same registrar, Jiangsu Bangning Science & Technology Co. LTD.



(https://www.arbornetworks.com/blog/asert/wp-content/uploads/2018/02/musical_chairs_CNCs.png)
The newest domain, etybh[.]com, was registered in December of 2017. Looking at PassiveTotal, all three domains appeared to have switched from 98.126.223.218 to 45.34.148.146 sometime in the middle of January 2018. This is our first clue that they are related.

Association No. 2

This one comes from looking at behavior when the file is attached to a debugger. First, let us back up a step. Observing behaviors of our suspected Musical Chairs Gh0st sample via a sandbox, we see that it creates a folder called “Win32Tetris”. Let’s see if there are any other Gh0st samples that do this as well. Taking a look through ASERT’s malware corpus we find this sample, 11fe12bbb479b4562c1f21a74e09b233ed41c41b7c4c0cad73692ff4672fb86a, which also creates that folder. Using clues left by another researcher[ii], we can confirm that this more recent sample is from the Musical Chairs group due to the C2 and some other characteristics we’ll go over. The most promising correlation is that this sample’s C2 is www.yourbroiler[.]com which is a known C2 for this actor. Next, we find similarities from a different dropped file called C:\microsoft\lib\ki\vv.js whose content reads as such:

```
var ji;
new ActiveXObject('Wscript.Shell').Run('cmd /c rundll32
c:\\microsoft\\lib\\.\\ki\\Piano.ocx mystart',0);
```

(https://www.arbornetworks.com/blog/asert/wp-content/uploads/2018/02/vv_js_snippet.png)

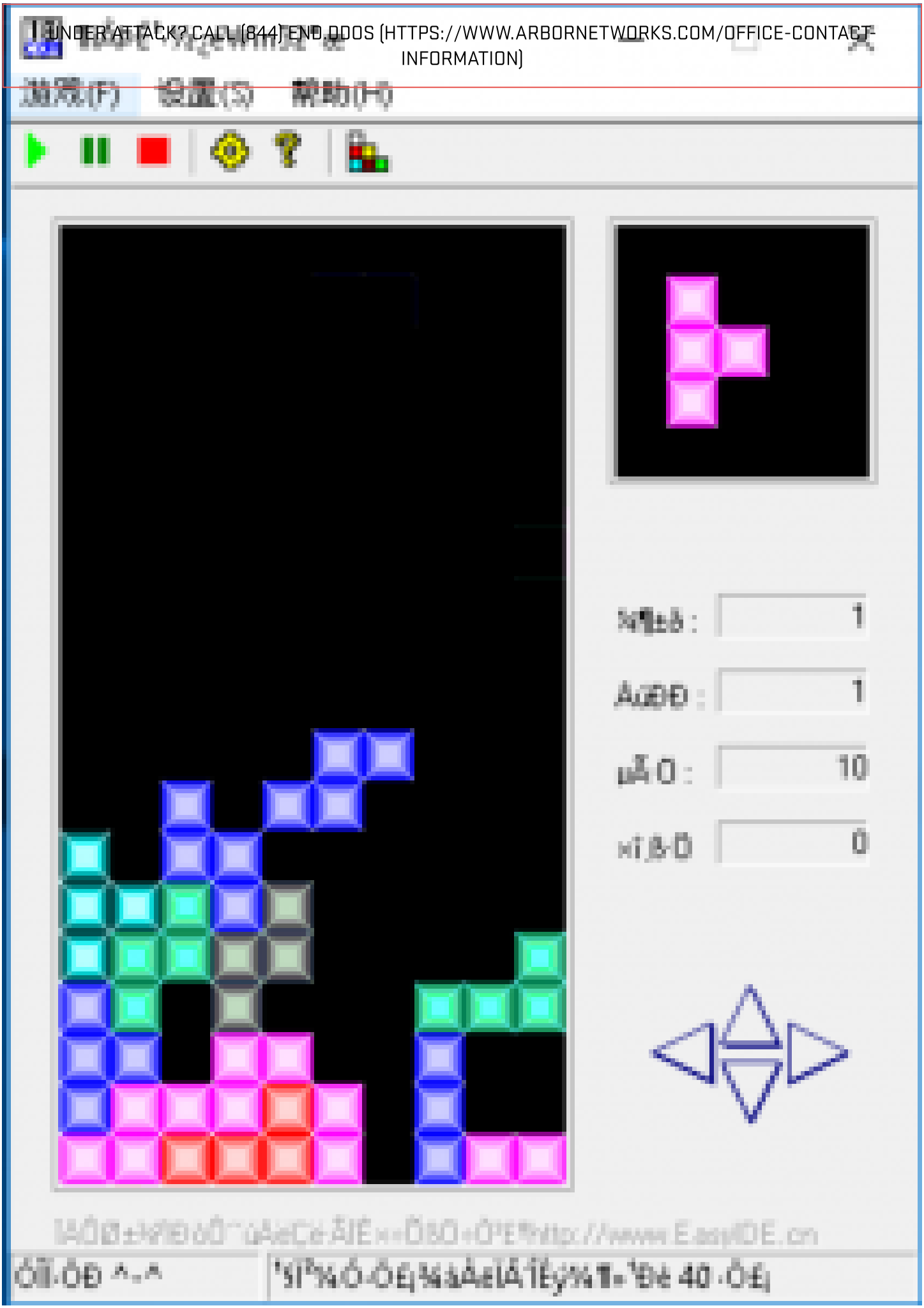
The content is similar to samples identified back in 2015[iii], which also used rundll32 to call a *mystart* method. And, finally, this sample makes use of the same mutex tied to this actor's Gh0st variant: dafewewrw.

To summarize the pivot sample

Property	Value
Load the dll via a script file called	C:\microsoft\lib\ki\vv.js
Domain	www.yourbroiler[.]com
Mutex	dafewewrw

Now that we have confirmed that this sample appears to be a Musical Chairs actor Gh0st variant, let's work the pivot (going to refer to this sample as the "pivot" sample).

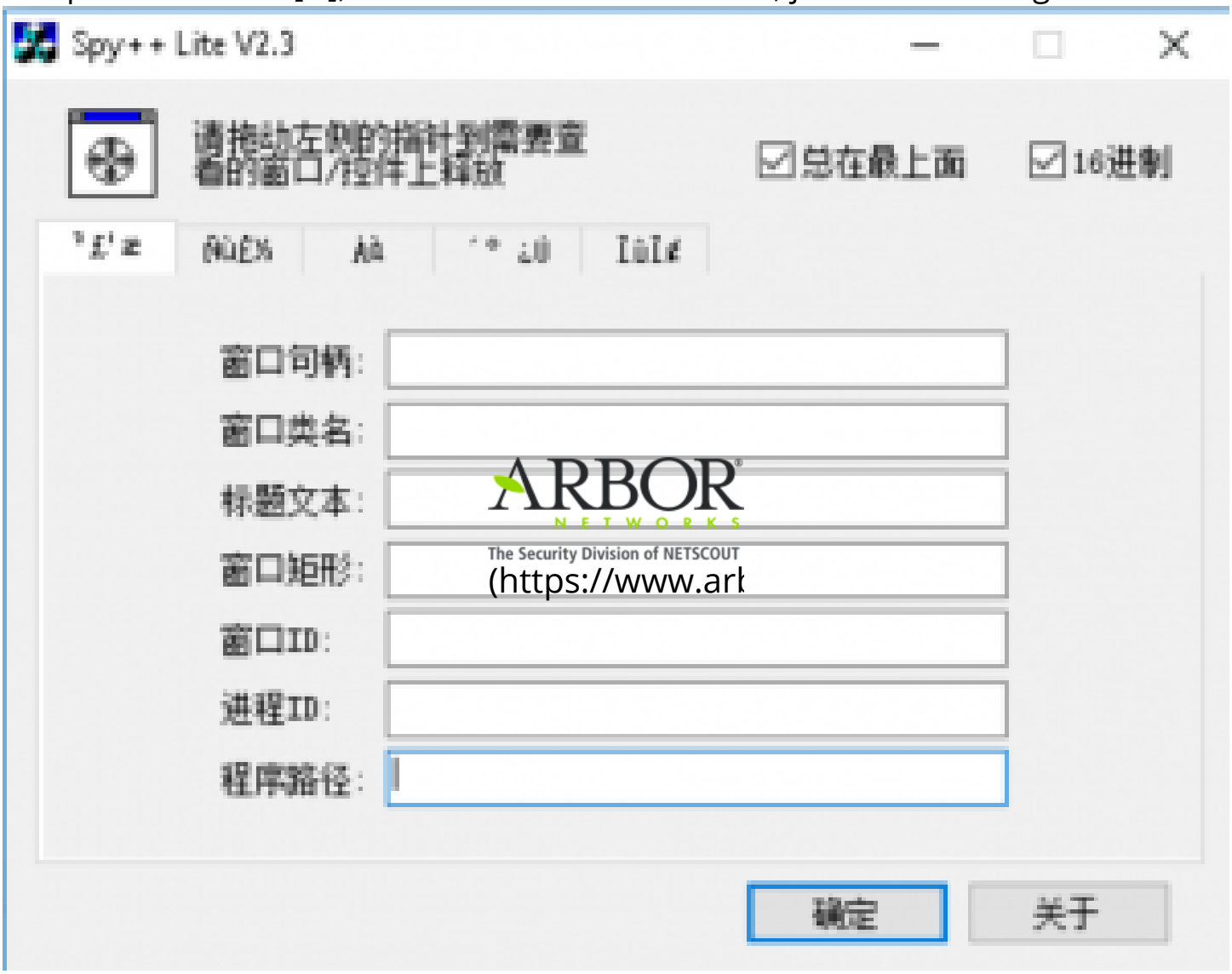
The pivot sample, when attached to a debugger, will launch what appears to be a fully functional Tetris game (very friendly of them to provide us reverse engineers with a short break):



(https://www.arbornetworks.com/blog/asert/wp-

content/uploads/2018/02/tetris.png)

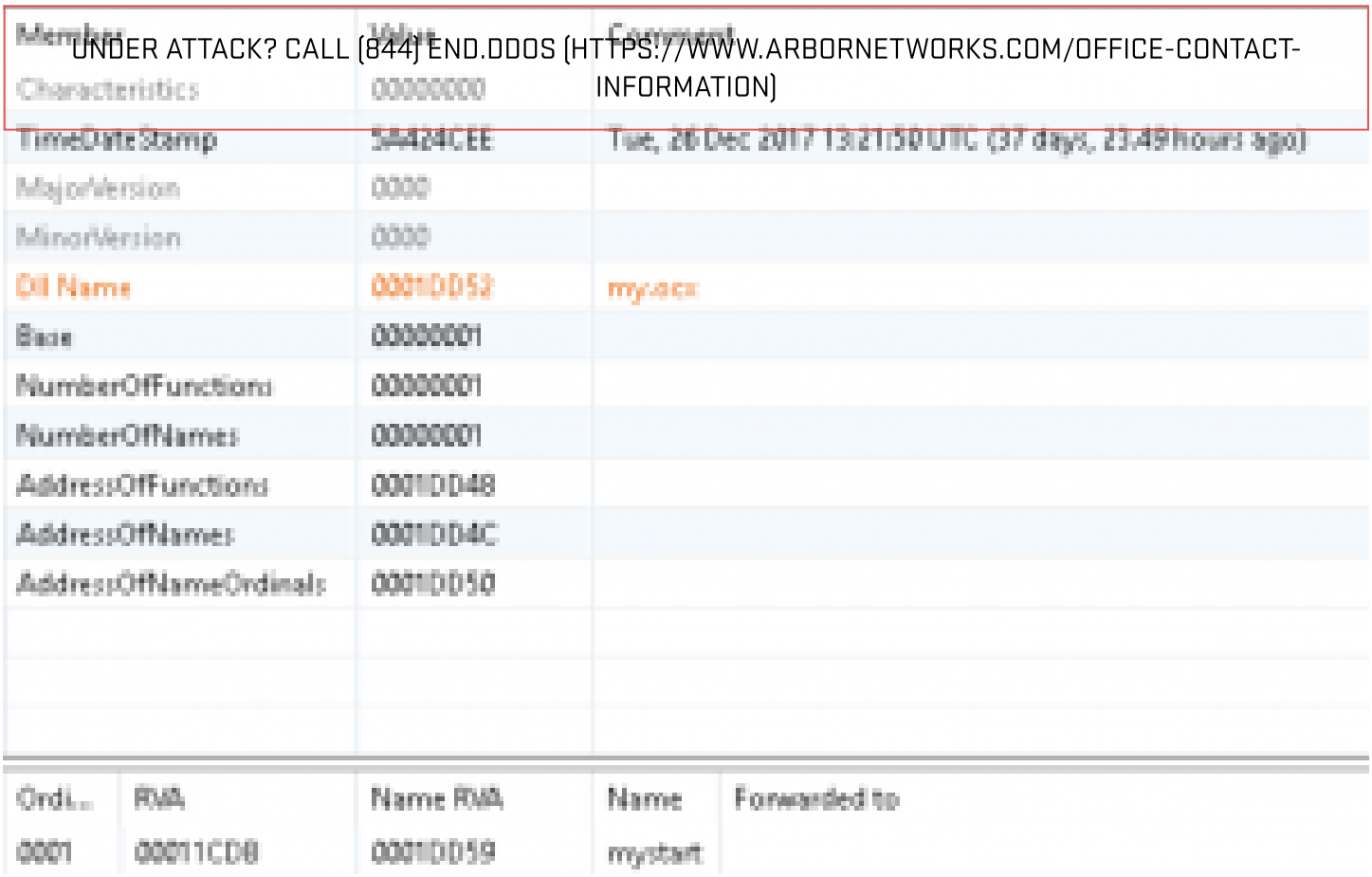
The latest sample (the one tied to the new domain, etybh[.]com) also exhibits this same behavior when attached to the debugger. To play the game make sure to not hide the PEB. For what it is worth, after checking out one of the prior samples from 2015[iv], it exhibited similar behavior; just not a Tetris game.



(https://www.arbornetworks.com/blog/asert/wp-content/uploads/2018/02/spy_lite.png)

Association No. 3

The final observation is the fact that the payload dropped on the file system as RasTls.dat is in fact an obfuscated DLL file. When looking at the DLL properties the *mystart* function is exported. Again, *mystart* is the exported DLL function which the samples back in 2015 called.



(https://www.arbornetworks.com/blog/asert/wp-content/uploads/2018/02/dll_properties.png)

Conclusion

While it should not surprise us when a long-standing actor switches things up, this specific actor is known for not really changing much. The use of a different Gh0st variant in addition to the new domain may be indicative of additional changes coming or the actor may be just keeping up with the times. Given previously observed behavior, it is likely that this indicator will be used in the campaign for the foreseeable future and ASERT is making it available to enable visibility for the broader security research community.

[i] https://researchcenter.paloaltonetworks.com/2015/09/musical-chairs-multi-year-campaign-involving-new-variant-of-gh0st-malware/

[ii] https://researchcenter.paloaltonetworks.com/2015/09/musical-chairs-multi-year-campaign-involving-new-variant-of-gh0st-malware/

[iii] https://researchcenter.paloaltonetworks.com/2015/09/musical-chairs-multi-year-campaign-involving-new-variant-of-gh0st-malware/

[iv] Hash: 50f08f0b23fe1123b298cb5158c1ad5a8244ce272ea463a1e4858d12719b337f

Posted in analysis (https://www.arbornetworks.com/blog/asert/category/analysis/), Malware (https://www.arbornetworks.com/blog/asert/category/malware/) | No Comments (https://www.arbornetworks.com/blog/asert/musical-chairs-playing-tetris/#respond)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

POST COMMENT

« The ARC of Satori (https://www.arbornetworks.com/blog/asert/the-arc-of-satori/)

SUBSCRIBE TO THIS BLOG

FIRST NAME

LAST NAME

COMPANY

EMAIL

UNDER ATTACK? CALL (844) END.DDOS (HTTPS://WWW.ARBORNETWORKS.COM/OFFICE-CONTACT-INFORMATION)

SUBSCRIBE

ASERT

Arbor's Security Engineering & Response Team (ASERT) delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as 'super remediators' and represent the best in information security.

Show more

Tag Cloud

"End of Internet" (https://www.arbornetworks.com/blog/asert/tag/end-of-internet/) Analysis (https://www.arbornetworks.com/blog/asert/tag/analysis/) Antiy (https://www.arbornetworks.com/blog/asert/tag/antiy/) APT (https://www.arbornetworks.com/blog/asert/tag/apt/) Arbor Networks - DDoS Experts (https://www.arbornetworks.com/blog/asert/tag/arbor-networks-ddos-experts/) Armageddon (https://www.arbornetworks.com/blog/asert/tag/armageddon/) Banking Trojans (https://www.arbornetworks.com/blog/asert/tag/banking-trojans/) BGP (https://www.arbornetworks.com/blog/asert/tag/bgp/) Bot (https://www.arbornetworks.com/blog/asert/tag/bot/) Botnet (https://www.arbornetworks.com/blog/asert/tag/botnet/) Botnets (https://www.arbornetworks.com/blog/asert/tag/botnets/) Buhtrap (https://www.arbornetworks.com/blog/asert/tag/buhtrap/) CAC (https://www.arbornetworks.com/blog/asert/tag/cac/) China (https://www.arbornetworks.com/blog/asert/tag/china/) Crypto (https://www.arbornetworks.com/blog/asert/tag/crypto/) CSAC (https://www.arbornetworks.com/blog/asert/tag/csac/) Danny McPherson (https://www.arbornetworks.com/blog/asert/tag/danny-mcpherson/) ddos (https://www.arbornetworks.com/blog/asert/tag/ddo Denial-of-service attack (https://www.arbornetworks.com/blog/asert/tag/denial-of-service-attack/) Dirt Jumper (https://www.arbornetworks.com/blog/asert/tag/dirt-jumper/) DNS (https://www.arbornetworks.com/blog/asert/tag/dns/) down (https://www.arbornetworks.com/blog/asert/tag/down/) Facebook (https://www.arbornetworks.com/blog/asert/tag/facebook/) Financial Sector (https://www.arbornetworks.com/blog/asert/tag/financial-sector/) Google (https://www.arbornetworks.com/blog/asert/tag/google/) Halloween (https://www.arbornetworks.com/blog/asert/tag/halloween/) hijack (https://www.arbornetworks.com/blog/asert/tag/hijack/) internet (https://www.arbornetworks.com/blog/asert/tag/internet/) Internet Protocol (https://www.arbornetworks.com/blog/asert/tag/internet-protocol/) Internet service

provider.

(https://www.arbornetworks.com/blog/asert/tag/internet-service-provider/) Internet traffic (https://www.arbornetworks.com/blog/asert/tag/internet-traffic/) IPv4 (https://www.arbornetworks.com/blog/asert/tag/ipv4/) IPv6 (https://www.arbornetworks.com/blog/asert/tag/ipv6/) Iran (https://www.arbornetworks.com/blog/asert/tag/iran/) malware (https://www.arbornetworks.com/blog/asert/tag/malware-2/) network (https://www.arbornetworks.com/blog/asert/tag/network/) outage (https://www.arbornetworks.com/blog/asert/tag/outage/) peering (https://www.arbornetworks.com/blog/asert/tag/peering/) Russia (https://www.arbornetworks.com/blog/asert/tag/russia/) Security (https://www.arbornetworks.com/blog/asert/tag/security/) Streaming media (https://www.arbornetworks.com/blog/asert/tag/streaming-media/) traffic (https://www.arbornetworks.com/blog/asert/tag/traffic/) Ukraine (https://www.arbornetworks.com/blog/asert/tag/ukraine/) Wikileaks (https://www.arbornetworks.com/blog/asert/tag/wikileaks/) YouTube (https://www.arbornetworks.com/blog/asert/tag/youtube/)

(http://arbor.link/ntctwww) Website (http://arbor.link/ntctwww) | **Blog** (http://arbor.link/ntctblog)