Malware

Musical Chairs: Multi-Year Campaign Involving New Variant of Gh0st Malware

By Brandon Levene, Robert Falcone and Jen Miller-Osborn
September 8, 2015 at 12:15 PM
Category: Malware, Threat Prevention, Unit 42
Tags: AutoFocus, Gh0st, Gh0stRat, Musical Chairs, Piano Gh0st, WildFire

The Gh0st malware is a widely used remote administration tool (RAT) that originated in China in the early 2000s. It has been the subject of many analysis reports, including those describing targeted espionage campaigns like Operation Night Dragon and the GhostNet attacks on Tibet. Musical Chairs is a multi-year campaign which recently deployed a new variant Gh0st we've named "Piano Gh0st."

Our evidence suggests the actors behind these attacks have been operating for over five years and have maintained a single command and control server for almost two. They use compromised e-mail accounts to distribute their malware widely and their targeting appears opportunistic rather than specific.

The overall motivation of this campaign is unclear at this time. Gh0st is very versatile as it allows an adversary to take complete control over the infected system including installing additional malware.

Tracking the Gh0st

Using Palo Alto Networks AutoFocus we have identified Gh0st variants associated with Musical Chairs leading back to mid 2013. The source code and building tools for Gh0st are available freely on the web; anyone who is so inclined can build their own version of the malware. The way researchers differentiate between most variants is based on their "magic tag."

Gh0st uses a custom TCP protocol to connect to a command and control (C2) server and retrieve instructions from the attacker. The malware identifies itself to the server by sending a string of characters (the magic tag), which the server repeats back to confirm the connection (See Figure 1.)

In the original version this string was "Gh0st" but in subsequent versions many different strings are used. These strings, along with the actual location of the command and control server (domain and/or IP address) allow us to associate various Gh0st samples with a single

attacker or group. In 2011, Norman released a paper that showed many clusters of Gh0st samples that were connected based on these tags.

Figure 1. Gh0st “magic tag” value sent over custom TCP protocol

Using these tags in the network traffic, the command and control infrastructure and other characteristics of the attacks, we have grouped together a series of attacks into the one campaign, named Musical Chairs.

The functionality of Gh0stRat (3.6) is well documented by multiple sources and is summarized below:

- Keylogging
- Remote terminal access
- Remote audio and video access
- File management
- Remote file download and execution
- Process explorer and additional system enumeration capabilities
- GUI interaction (remote control)
- Self Update
- Reset of SSDT to remove existing hooks

Spreading the Gh0st

The Gh0st variants used in the Musical Chairs campaign are distributed using phishing e-mails. The threat actors behind the attacks use a “shotgun” approach, blasting e-mails to as many recipients as possible in hopes of tricking a small percentage of targets into opening the attack. The attackers generally do not rely upon any vulnerability exploitation, and instead rely on the user to open the attached executable to compromise their system. Additionally, the phishing messages are sent from US-based residential ISP e-mail addresses. The accounts themselves appear to be legitimate, and are likely also compromised by this actor. In many cases the phishing e-mails are sent indiscriminately to all e-mail addresses in an infected user’s address book, including “no-reply” addresses a human operator would know to ignore.

While Gh0st itself does not have built in e-mailing components, it is also possible that an additional payload is responsible for the propagation via e-mail.

The following list contains known filenames of attachments used in the delivery stage of the Musical Chairs campaign:

- “Pleasantly Surprised.exe”
- “Beautiful Girls.exe”
- “Sexy Girls.exe”
- “gift card.exe”
- “amazon gift card.pdf.exe”

The subject of the e-mails carrying these files typically matches the filename itself and does not contain any sophisticated attempts at social engineering. The attacks detected thus far by Palo Alto Networks WildFire have been exclusively in the United States and do not appear to target any particular industry.

Infrastructure

The infrastructure used in Musical Chairs stands out primarily due to its longevity and use of multiple Gh0st command servers on the same host. At the center of the infrastructure for the last two years is a Windows 2003 server using the IP address 98.126.67.114. The server uses a US-based IP address, but displays a Chinese language interface for Remote Desktop connections.

Figure 2. Chinese language Windows Server 2003 login banner on Gh0st C2

Thus far Unit 42 has identified 32 different Gh0st samples connecting to this server dating back to July of 2013. The Gh0st C2 software operates on Windows and allows the attacker to specify which port it should listen on for connections from infected systems. The attacker may host multiple Gh0st C2s on this server at one time, or may change the hosting TCP port very frequently. The 32 samples we have identified connect to 19 different TCP ports.

First Seen	Gh0st TCP Port
7/18/13	10003
9/4/13	10009
9/4/13	10008
9/14/13	10004

10/15/13	10004
11/21/13	20004
11/28/13	20001
1/2/14	40000
1/2/14	40000
1/9/14	20004
1/29/14	10008
3/17/14	30001
4/17/14	8001
4/22/14	8001
7/14/14	10005
8/18/14	8003
9/10/14	9000
9/19/14	9000
10/27/14	10006
2/20/15	9001
3/24/15	600
7/13/15	200
7/15/15	200
7/15/15	200
7/17/15	200
7/21/15	200
7/21/15	201
7/22/15	201
7/29/15	201
8/10/15	203
8/18/15	204
8/20/15	204

While 98.126.67.114 is the longest standing command and control server, it is not the only server used by Musical Chairs. The malware typically finds this server using a domain that is registered by the attacker and the registration information used by these C2 domains has allowed us to identify additional infrastructure used in these attacks.

Figure 3. Diagram of relationships between Musical Chairs C2 domains and related infrastructure

These many related domains put the approximate start date of this campaign in 2010. The earliest versions of the attacks we've found are still visible in e-mail groups and public Facebook postings. Figure 4 shows an e-mail with the subject "my girlfriend's self-view video" that contains a link to an executable hosted on nvzm.info, one of the domains associated with the Musical Chairs infrastructure.

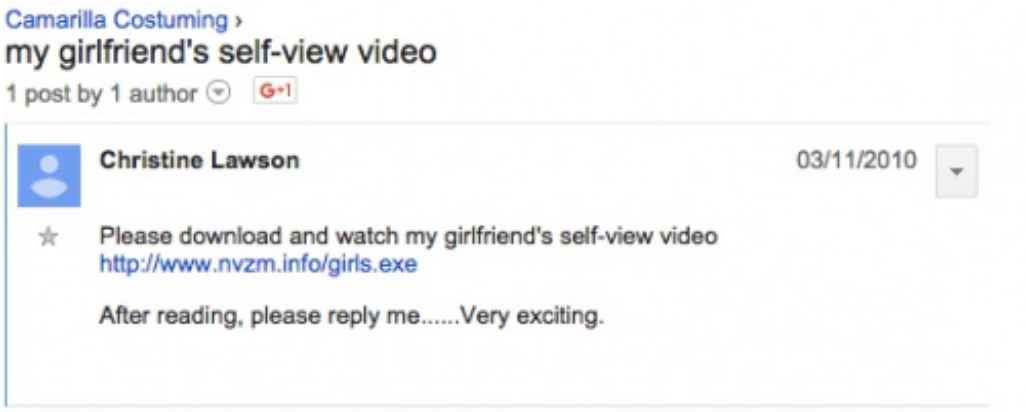

Figure 4. Screenshot of e-mail linking to nvzm[.]info using a "self-view video" theme.

The image below shows a Facebook post from 2012 with a similar theme and a different link

to a URL that is also part of the same infrastructure map.

Figure 5. Screenshot of Facebook posting including a different “video” theme.

Finally, we located a user who posted to the Gmail Help forum in 2010 requesting assistance with ridding their system of malware. He states that all of his contacts received one of the “self-view” phishing e-mails after his system was compromised.

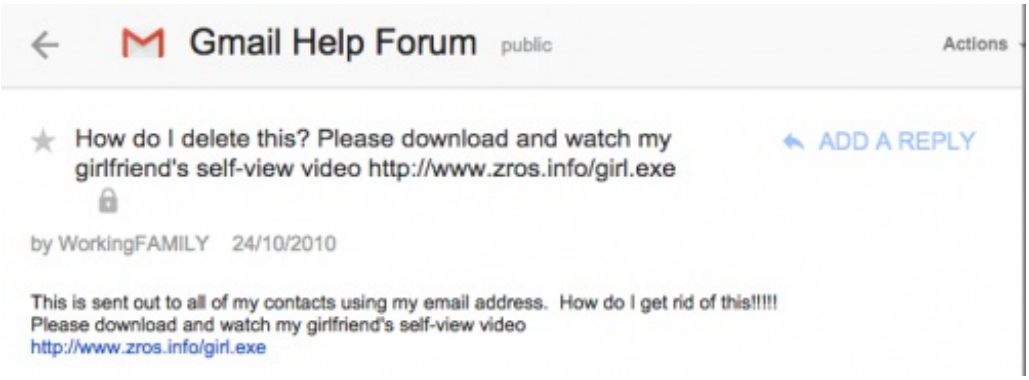

Figure 6. Screenshot of request on Gmail help forums related to “self-view” video e-mails.

While we have not been able to identify the specific malware used to distribute these spam messages, the infrastructure and the themes used in the e-mails connect them directly back to Musical Chairs happening this year.

Piano Gh0st

In July, Musical Chairs began deploying a new variant of Gh0st, which we’ve named “Piano Gh0st.” This variant uses a new wrapper file to hide the Gh0st payload. The files are delivered as a self-extracting executable (SFW) that acts as the dropper. It is responsible for extracting its payload to “c:\microsoft\lib\ke\Piano.dll” and executes the “mystart” function within the DLL’s export address table (EAT) using rundll32.exe.

Figure 7. Screenshot of calls observed by Palo Alto Wildfire from within the AutoFocus interface.

The “Piano.dll” file itself has very little functionality other than decrypting, loading and running an embedded DLL. It decrypts the embedded DLL using the Blowfish symmetric cipher with a simple key consisting of the character “y”. “Piano.dll” proceeds to load the newly decrypted DLL manually and calls the exported function “my start”. The decrypted DLL has the following attributes:

MD5: 8182a33cc1268c0c3b4e3d9a02d912c9

SHA256: 32026e702cff8fd3f113473ea2698eab0ca181aa2d0fd0e8802e31aa3befa94a

Type: PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit

Size: 148008 bytes

Imphash: 9c01d71c9bf78d231a313c86540e284c

Compiled: 2015-07-14 02:11:32

Exports:

(0x123f0) mystart

This embedded DLL is the actor Gh0stRat Trojan, specifically version 3.6. The following debugging path is found within the DLL, which suggests the individual who compiled this DLL has a Chinese language pack (GB2312 specifically) installed:

C:\Documents and Settings\Administrator\桌面\GetRawInputData_dlll键盘记录版_win7bug改_网络验证_Mutext_LSPlayer_20150708\gh0st3.6\Server\svchost\Release\

The Trojan maintaings persistence on the infected system by creating an entry in the registry at “HKCU\Software\Microsoft\Windows\CurrentVersion\Run” with the key “nvidiake” and value “c:\microsoft\lib\ke\vv.js”, as seen in Figure 8.

rundll32.exe	RegSetValueEx	HKCU\Software\Microsoft\Windows\CurrentVersion\Run , nvidiake , microsoft\lib\ke\vv.js
rundll32.exe	SetValueKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\nvidiake , Value:microsoft\lib\ke\vv.js , Type:1

Figure 8. AutoFocus view of registry key modifications made by Piano Gh0st to maintain persistence through system reboots

The file “vv.js” in the registry key is a simple one-line JavaScript that executes the “vvv.bat” file, as seen in the following:

```
1 new ActiveXObject('Wscript.Shell').Run('cmd /c c:\\microsoft\\lib\\ke\\vvv.bat',0);
```

The ‘vvv.bat’ file is a batch file that executes the Piano.dll payload in the same way as the initial dropper, using “rundll32.exe” to call the “mystart” exported function, as seen in the following:

```
1 rundll32.exe  c:\microsoft\lib\ke\Piano.dll mystart
```

After setting up the registry keys for persistence, the Gh0stRat sample begins communicating with its command and control server using a custom network protocol. The magic tag used by this version of Gh0st is “clarkclar1” as seen in Figure 9. This variant also communicated with a command and control server using the domain www.meitanjiaoyiwang[.]com, which is hosted by 98.126.67.114 on tcp port 200.

```
00000000  63 6c 61 72 6b 63 6c 61  72 31 00 00 00 54 e0 00 clarkcla r1...T..
00000010  00 00 78 9c 4b 63 67 60  98 c3 c0 c0 c0 0a c4 8c ..x.Kcg` ........
00000020  40 ac c1 c5 c0 c0 04 a4  83 53 8b ca 32 93 53 15 @....... .S..2.S.
00000030  02 12 93 b3 15 8c 19 e8  0e 98 41 04 23 23 d8 3d ........ ..A.##.=
00000040  07 56 6c d1 cc 2b cd c9  21 d5 0c 5b 0e 06 06 00 .Vl..+.. !..[....
00000050  a5 0a 0a 83                                      ....
```

Figure 9. Screenshot of Piano Gh0st variant using the “clarkclar1” magic tag.

Detection and Prevention

Palo Alto Networks WildFire detected the Gh0st malware, including the Piano Gh0st variant, as malicious based on the behavior the attack files exhibit on an infected system.

Additionally, we have deployed threat prevention signatures to detectPiano Gh0st alongside our previously deployed signatures for earlier Gh0st variants. AutoFocus users can find more

information about this threat using the MusicalChairs tag.

The following indicators identify attacks using Piano Gh0st and the Musical Chairs campaign.

type	value
sha256	50f08f0b23fe1123b298cb5158c1ad5a8244ce272ea463a1e4858d12719b337f
sha256	8dac9fa1ea29a90893a77f4d49c1393fa99a967e8af6a507037789041911de95
sha256	f08f26a7026ba249d021ca21f097405a536771f38d94081731c0f7960177408b
sha256	f5c868d9ac4d18c9c88e181af9370769bf52928d04874d8c3142badf83f664e3
sha256	e60c25ee1404433e3f78e50f5edea11f186211148ce8e5abb22c1f01b76d96f3
sha256	4babcaf4694fb8207ea3774f6c2339a28c0ce5913fb9ac396a8e50efa75e10cd
sha256	d36d80c5b9da830fd027cd219d9dabcedd73f5d2da5009b2661c4f0438773c3e
sha256	29726da0ebd8960cab09f91bb8fa37db27b1ca2a3897235c645d1896df10303b
sha256	61b77cada9c2a16daeb465e439cb3e38c857f15594551874698219 3bf542666
sha256	a0fdb977b712e669aae28723f1a4b90735a5af9e92937558c9da8f62614a1a17
sha256	73ae929dde6826306046d8db744da6e5150f5c508298726b634d39c279192ad0
sha256	e297929c583c6f84727c312b937c43550d71fe2bca4f4138d53441c7e269cfa4
sha256	55090a930b6c37f9ff215793e950a4ffb67f516fd0a14409b027f995d27da082
sha256	a7afee2227ff3ee64695235c7eed214ee1d18c2b6e287616118b5f38fd6720dc
sha256	4306af9aa2b585dd07c4b114bc7e292f7f9ab06732ae7a9e7f4831b88127c85a
sha256	66b1260565e2243bba1436f43e986ff741bd391305114d7bef891273e03abd72
sha256	022ca8187bfb1f347a0e547417a8088a5cc0e38fd9aa51b464154fbcf4aa149c
sha256	9b823f0d60e348707fbbc1da8b37b3c9cd5ea1f43277ba8069e302ff05fee531
sha256	c256ca3514d23818cab28b61d1df52a513d1f2beda8c5e81c3336de762f9f3f4
sha256	7eeba4a511cdeb6b48ca3d09b751be047aa553ea5f6c416494200d1aee520fe4
sha256	552ff44540e944b3263fc8c32c7dba927f6e7f3f4489bb13b8ecc52c3fd40bf1
sha256	e1290e92c5caff9631f4ebe53df27293b71df19b6b5435323332658ebaa9c6b6
sha256	fb8b4bc012d45ba78e721a6f73df77ac7838998109c388ced95c995a7e7303f8
sha256	20236c7a6c0c29664976ab943118477583545ed8461b14933b2d49cee10dd051
sha256	da297e8bf799032e0a52c4535997abf30202f33ce9d4162139129463c386efcc
sha256	4b7133e45f368cc0b6728830bc9e1219ff318eb384caf5ecbb54e12e6e6c1925
sha256	e737e2253f016ab65b521d4f4e7b2a06741fa2541c52f0994edfc1763a053910
sha256	07cf20da1ef235ee98c25495bf9b845754f21ed105d5211001885fd2eea3210f
sha256	d467504e8b8608b4fae334c426e8ac02f762993064bf1db20bb6090b42648648

sha256	8a2a5f155707109bc0a6f179f1a749b216504b373c765c8193a7dd958b17be7c
sha256	a95933553fca054e08bd213b7f364b084ef19936a425d7260e08a8e7fdfd2ce6
sha256	6adced734d5498bbcc9fc111ce43bd7fd8db098106eaa3cfc025de7ba6dc02a7
sha256	c608bb6f3723aad1608963e661c8fb80ace93f02f7d52f61a1355e9512676d62
sha256	e58085656708d9759856325afb6cd67ec0ff7a126e27907efa2e91ef9a0ff474
sha256	bba343d4043ea3d170f4027546fad7f991b7ebce9e923dc42e16d88b570ff167
sha256	96c301bfa09338740575c4758d558b12e338654b16fc4b9d2badb9610358bf63
sha256	d3c8161f76d4187f32039b5557e22e5fb684c06aa3e145e813ee7a4e166cbf47
sha256	34dabb10ea595c773ae4f8c13b7d7fdb41927bc7052ef76204735bbffeda1c47
sha256	9c547a7c523e367948d2c645407d0919053ef48292173efe263f3ccfdcdc8e92
sha256	f31b23dee1e047e5b472bca54c06594c2cca5adcebd2290f35b60cb2ebb3ee26
sha256	a764f76276e41ec49b388e8c7c53b602edcc29ff3ac8f8ab4b52913eb91934e3
sha256	e58eb692d3933dfda630f659d447d7c8026eaf32d35478bd7056515706eb1481
sha256	b50544ad3341fbee60338f45bd4043450238a301e022c1010115a2003a970a23
sha256	09f24435e47be74f90d032c78a84fa37f06ce9452a6d3a75c263ae012a7ae626
sha256	83e7aaf52e5f567349eee880b0626e61e97dc12b8db9966faf55a9921bac61da
sha256	acc340d986e720441ec5112746d3f94b248b44fe5d4c1da0fb866a3013384ad2
sha256	1181e9bb8fbcf1ebad8b6a7f157b6cc71e9c996c3601baecc3a2f25ba27032ee
sha256	89968a9c846aad54cd78d7bfe704f0ab71f75d54b982540f594afdaa9100f4fc
sha256	88feda3120381216bc96a09e4b6e43e89d5776b5ca3b2d820710be0678f19867
sha256	f37dc918d8064671edcb28c12397c576d3b66b6da21e1670a1a9428f03fb8478
sha256	3a8ddb7b456332301d02222df48070f62e1e39a48e74f39ca8633028599ae250
sha256	7b8a3efef6c4847697331badcdb0b306ceaa013233ce1c7ee8de8ae933c2d89d
sha256	ca63a159d58cb7b9bff57646b0e5bc9a61c51f4e08304d9d73c87c876f77b7f5
sha256	76d97074410251347a9398a90e42e02866c30ba71303fe9cccf236ea229172a4
sha256	c76a817bcae00ec0ca86624b2e62458fec07a5682d92eb59568639fa0586bb1e
sha256	bdb89defb03055e962c6627e8baa0ffd83dda81a1b239bc48e751c2ea5aa2b29
sha256	81c8ef33d1e6ebfaad55e20b1e715007aa310b6aa55903e427225648efbbb779
sha256	85894b6181535efe15ec5ff7575cee8975aa86ec611d94fb7709b54e5ccfc9f2
sha256	ed25e3d5c13f409242ded579c45f9c4bb4416c204e1ee16cf63f744cf2ccd62c
sha256	a34f37c19785b029bf690d53b89f910586660fb94abd8587bfe110c3db6856bc
sha256	20299a5fc850ec4cd1aceb7cf1987609c05fa08d59dd5ae79e15bc048c46685e

domain	meitanjiaoyiwang[.]com
domain	yourbroiler[.]com
ip	98.126.67.114
ip	68.68.105.174
ip	98.126.121.202
ip	173.254.223.24
mutex	Global\\dafewewrw
filename	Piano.dll
filename	Beautiful Girls.exe
filename	Pleasantly surprised.exe
filename	amazon gift card.pdf.exe
filename	Sexy Girls.exe
filename	vv.js
filename	vvv.bat
email address	596552@qq.com

Got something to say?

Leave a comment...

Notify me of followup comments via e-mail

Name (required)

Email (required)

Website

SUBMIT

SUBSCRIBE TO NEWSLETTERS

Email SUBSCRIBE

COMPANY

Company

Careers

Sitemap

Report a Vulnerability

LEGAL NOTICES

Privacy Policy

Terms of Use

ACCOUNT

Manage Subscription

SALES > 866.320.4788 »

SEE A DEMO »

TAKE A TEST DRIVE