Trend Micro Incorporated
Research Paper
2012

# The HeartBeat APT Campaign

Roland Dela Paz

## Contents

About This Paper ........ 1
Introduction ........ 1
Campaign Targets ........ 2
Context ........ 2
Attack Vector ........ 3
Infection Flow ........ 4
The RAT Component ........ 5
    Backdoor Functionalities ........ 5
    Installation and Persistence ........ 5
    C&C Communication ........ 6
Command and Control ........ 8
HeartBeat Campaign Codes and Decoy Documents ........ 8
Relationships among C&C Domains, IPs, and Campaigns ........ 9
Attribution ........ 10
Conclusion ........ 10
Timeline ........ 10
Defending against the HeartBeat Campaign ........ 11
Trend Micro Threat Protection Against The HeartBeat Campaign Components ........ 12

## About This Paper

This paper exposes a targeted attack called "HeartBeat," which has been persistently pursuing the South Korean government and related organizations since 2009. This paper will discuss how their specifically crafted campaigns infiltrate their targets.

Compared to most advanced persistent threat (APT) campaigns with diverse targeted industries, the HeartBeat campaign is an isolated case. Furthermore, we will examine their attack methodologies which include their attack vector, the remote administration tool (RAT) component, and command-and-control servers. Finally, we will discuss how this information can be useful in developing defensive strategies in protecting organizations as well as predicting future targets.

## Introduction

Today's cybercriminals try to infect as many users as possible. Their goal is simple—to monetize the resources or data from infected machines in any way they can. Behind such attacks are highly covert targeted campaigns known as APTs.

While targeted campaigns continue to increase, research efforts by the security industry reveal that some of these attacks have existed for several years.[1] Depending on the motive, APT campaigns may attack various industries, organizations or communities from different regions and countries. For instance, the Luckycat campaign targeted the aerospace, energy, engineering, shipping, and military research industries in India and Japan.[2] Additionally, they targeted the Tibetan activists' community. The IXESHE campaign, on the other hand, targeted East Asian governments, Taiwanese electronics manufacturers, and a telecommunications company.[3] While most of these campaigns have multiple targets, smaller, more subtle campaigns with exceedingly specific targets are also present. The Taidoor campaign is an example of this, where all of the compromise victims were from Taiwan, and the majority of which were government organizations.[4]

This research paper will delve into a targeted campaign that targets organizations and communities within South Korea. We call this malicious operation the "HeartBeat campaign."

[1] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf

[2] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf

[3] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

[4] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf

## Campaign Targets

The HeartBeat campaign appears to target government organizations and institutions or communities that are in some way related to the South Korean government. Specifically, we were able to identify the following targets:

- Political parties
- Media outfits
- A national policy research institute
- A military branch of South Korean armed forces
- A small business sector organization
- Branches of South Korean government

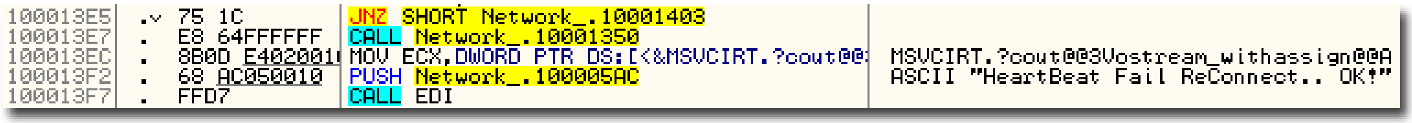
The profile of their targets suggests that the motive behind the campaign may be politically motivated.

## Context

The first HeartBeat campaign remote access tool (RAT)[5] component was discovered in June 2012 in a Korean newspaper company network. Further investigation revealed that the campaign has been actively distributing their RAT component to their targets in 2011 and the first half of 2012. Furthermore, we uncovered one malware component that dates back to November 2009. This indicates that the campaign started during that time or earlier.

Earlier versions of the HeartBeat campaign's RAT component contained the following strings in their codes:

Thus, the campaign name "HeartBeat."



```
100013E5  .v 75 1C          JNZ SHORT Network_.10001403
100013E7  .  E8 64FFFFFF    CALL Network_.10001350
100013EC  .  8B0D E402001(  MOV ECX,DWORD PTR DS:[<&MSVCIRT.?cout@@:  MSVCIRT.?cout@@3Vostream_withassign@@A
100013F2  .  68 AC050010    PUSH Network_.100005AC                   ASCII "HeartBeat Fail ReConnect.. OK!"
100013F7  .  FFD7           CALL EDI
```

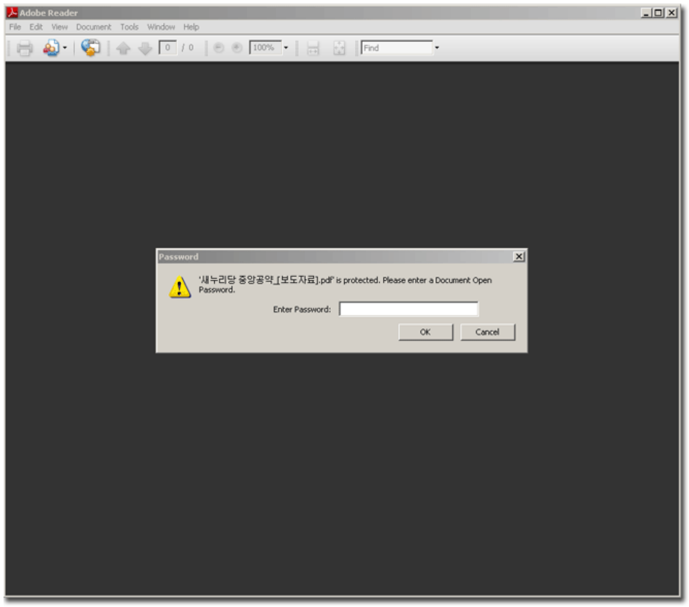
*Figure 1. Code used in the HeartBeat campaign's RAT component*

[5] http://en.wikipedia.org/wiki/Remote_administration_software

# Attack Vector

In order to gain control over targets systems, HeartBeat perpetrators install a RAT in prospective victims' systems. This RAT arrives as a disguised or fake document which is actually a bundled file. The bundled file contains both a decoy document and the RAT installer that has been packaged together using a binder tool. Once it runs, the decoy document is displayed to the user while the RAT unknowingly executes in the background.

It is unclear how these packaged files specifically arrive on victims' systems, but we highly suspect that spearphishing emails[6] containing these packaged malware were primarily used to distribute them. In fact, the packaged malware used the icon of the decoy document in order to look legitimate. For instance, if the decoy is an XLS file, the package will appear to have an XLS document icon. In addition, some of the decoy files required passwords in order to be viewed.



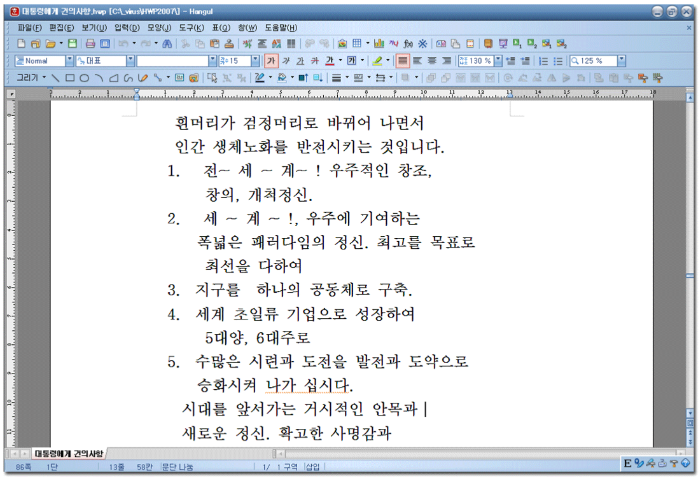
'새누리당 중앙공약_[보도자료].pdf' is protected. Please enter a Document Open Password.

Enter Password:

*Figure 2. Example of a decoy* Adobe Reader *document*

The previously mentioned techniques are commonly used in spearphishing attacks where prospective victims are lured to open a seemingly benign document attachment. In order to appear more legitimate, some of these emails contain password protected documents. A password is then provided in the email body as a social engineering technique.

Based on the samples we collected, the campaign's decoy documents used the file formats .JPG, .PDF, XLS, and HWP, the Korean government standard word processor format. One of the previous HeartBeat attacks even dropped a pornographic .JPG image as decoy. Below is a screenshot of a *Hangul Word Processor* (.HWP) document used as bait in November 2011. Its document title roughly translates to "*Information to the President.hwp*."


대통령에게 건의사항.hwp [C:_virus\HWP2007\] - Hangul
파일(F) 편집(E) 보기(U) 입력(D) 모양(J) 도구(K) 표(Q) 창(W) 도움말(H)
Normal
대표
15
130 %
125 %
그리기
대통령에게 건의사항
86줄 1단 13줄 58칸 문단 나눔 1/ 1 구역 삽입

흰머리가 검정머리로 바뀌어 나면서
인간 생체노화를 반전시키는 것입니다.
1. 전~ 세 ~ 계~ ! 우주적인 창조,
창의, 개척정신.
2. 세 ~ 계 ~ !, 우주에 기여하는
폭넓은 패러다임의 정신. 최고를 목표로
최선을 다하여
3. 지구를 하나의 공동체로 구축.
4. 세계 초일류 기업으로 성장하여
5대양, 6대주로
5. 수많은 시련과 도전을 발전과 도약으로
승화시켜 나가 십시다.
시대를 앞서가는 거시적인 안목과
새로운 정신. 확고한 사명감과

*Figure 3. A decoy .HWP document*

[6] http://blog.trendmicro.com/taiwan-spear-phishers-target-gmail-users/

## Infection Flow

Once users open the packaged malicious file, the actual document is displayed to the user while a RAT installer in .EXE format runs in the background. The RAT installer, on the other hand, drops a .DLL file that is then injected to the legitimate process svchost.exe. The injected code in *svchost.exe* then connects to the malware command and control (C&C) server to register infection and wait for remote commands.

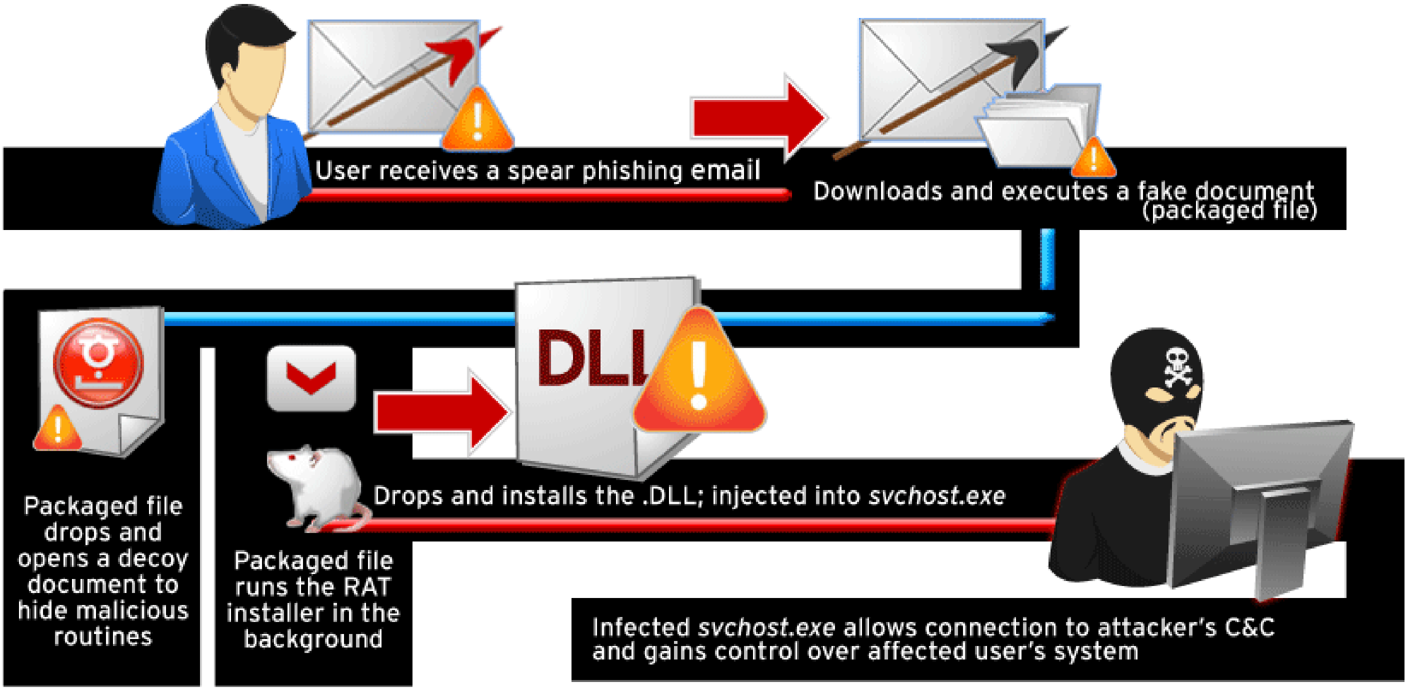

User receives a spear phishing email
Downloads and executes a fake document (packaged file)
DLL
Drops and installs the .DLL; injected into *svchost.exe*
Packaged file drops and opens a decoy document to hide malicious routines
Packaged file runs the RAT installer in the background
Infected *svchost.exe* allows connection to attacker's C&C and gains control over affected user's system

*Figure 4. Infection diagram for the HeartBeat campaign*

# The RAT Component

## Backdoor Functionalities

The HeartBeat campaign's RAT component allows attackers to remotely execute the following commands on affected hosts:

- List running processes and their respective process IDs
- Download and execute file(s)
- Update itself
- Uninstall itself
- Create or terminate a process
- List available removable and fixed drives
- List existing files and their creation date/time
- Upload file(s)
- Delete file(s)
- Get the file creation date/time of a specific file
- Open a remote command shell access
- Reboot the system

These commands give the attackers complete control over their victims' systems. Attackers also have the option to uninstall the RAT any time to cover their tracks and avoid being discovered.

## Installation and Persistence

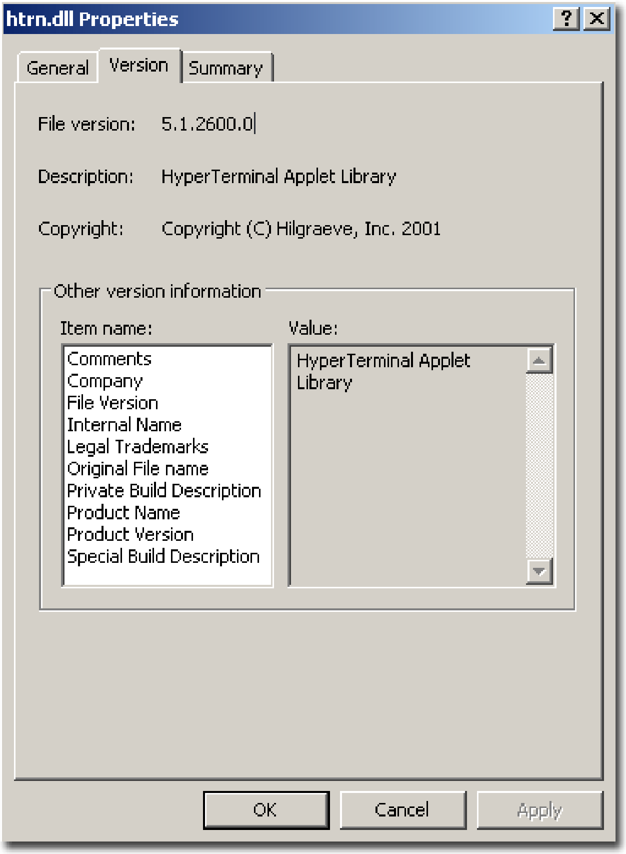
The RAT installer is initially dropped and executed by the packaged file using any of the following file names:

- *%System%\msrt.exe*
- *%Program Files%\Common Files\AcroRd32.exe*
- *%Program Files%\Common Files\config.exe*
- *%Program Files%\Common Files\explorer.exe*

The RAT installer in turn drops a .DLL component which contains the backdoor capabilities. In order to stay hidden, the .DLL uses file names similar to legitimate applications. Below is a list of file names used:

- *%Program Files%\Common Files\Services\6to4nt.dll*
- *%Program Files%\Common Files\System\6to4nt.dll*
- *%Program Files%\Windows NT\Accessories\6to4nt.dll*
- *%Program Files%\Windows NT\htrn.dll*
- *%Program Files%\Windows NT\htrn_jls.dll*
- *%Program Files%\Windows NT\hyper.dll*
- *%System%\Network Remote.dll*
- *%System%\SvcHost.dll*

Some these dropped .DLL files use fake file properties in order to not appear suspicious. The following is an example:



File version: 5.1.2600.0

Description: HyperTerminal Applet Library

Copyright: Copyright (C) Hilgraeve, Inc. 2001

Other version information

| Item name: | Value: |
|---|---|
| Comments<br>Company<br>File Version<br>Internal Name<br>Legal Trademarks<br>Original File name<br>Private Build Description<br>Product Name<br>Product Version<br>Special Build Description | HyperTerminal Applet Library |

*Figure 5. A.DLL that uses fake file properties*

In some cases, the RAT installer drops 2 .DLL files where one of the .DLLs serves as a loader of the other .DLL file which contains the backdoor payload.

The .DLL component is then registered as a service through the following added registries:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}
Type = "20"
Start = "2"
ErrorControl = "1"
ImagePath = "%SystemRoot%\System32\svchost.exe
-k netsvcs"
ObjectName = "LocalSystem"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}\Parameters
ServiceDll = C:\Program Files\Windows NT\htrn.
dll
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}\Security
Security = {values}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}\Enum
0 = "Root\LEGACY_{service name}\0000"
Count = "1"
NextInstance = "1"
*{service name} may be "6to4", "Ias" or
"Irmon".
```

The service is then invoked once installed. This results in the .DLL being injected to *svchost.exe* process. This registry modification allows the RAT to execute upon every system startup.

After installation the RAT installer deletes itself, which leaves only the disguised .DLL and related registry entries on the affected system.

Note that the presence of any of the files or registries above may be an indication of a possible HeartBeat infection in a system.

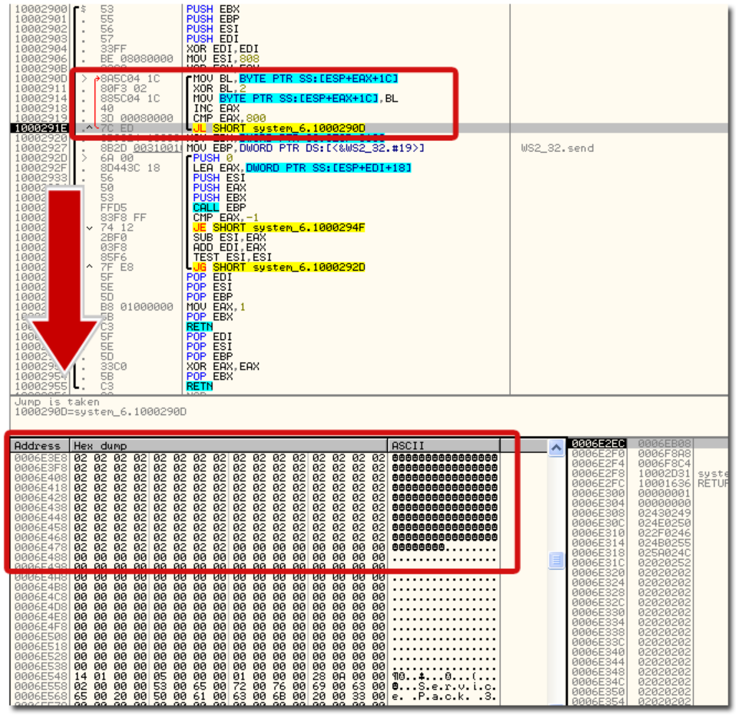
## C&C Communication

Once the RAT's .DLL component has been injected to *svchost.exe*, the malware attempts to register itself to the C&C server by sending the following information from the affected system:

- Computer name
- Local IP address
- Service pack

These data are sent along with a campaign code and the string "qawsed". While the "qawsed" string is not present in earlier versions of their RAT, we suspect that the attackers only recently added this as a default campaign password.

The RAT's C&C communication is encrypted with XOR encryption using a single byte key, 02H. Furthermore, the data being transferred and received by the RAT C&C are 800H (2,048 bytes) in size.



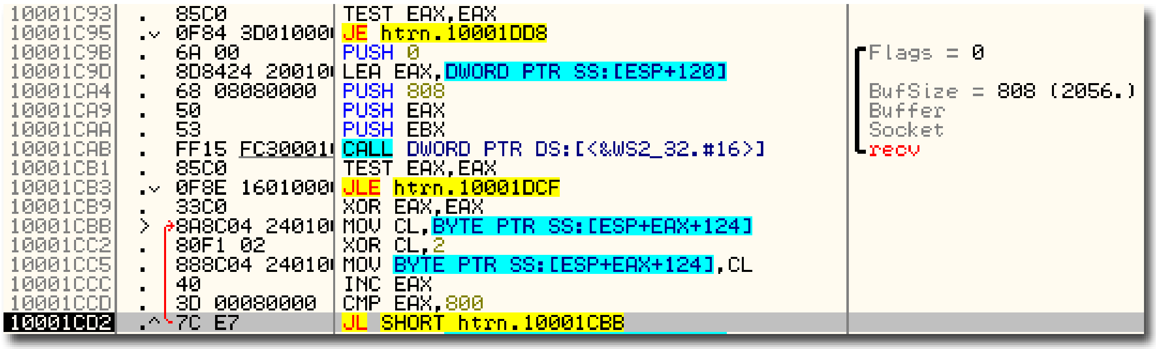
```
10002900  $  53            PUSH EBX
10002901  .  55            PUSH EBP
10002902  .  56            PUSH ESI
10002903  .  57            PUSH EDI
10002904  .  33FF          XOR EDI,EDI
10002906  .  BE 08080000   MOV ESI,808
1000290B
1000290D  >  8A5C04 1C     MOV BL,BYTE PTR SS:[ESP+EAX+1C]
10002911  .  80F3 02       XOR BL,2
10002914  .  885C04 1C     MOV BYTE PTR SS:[ESP+EAX+1C],BL
10002918  .  40            INC EAX
10002919  .  3D 00080000   CMP EAX,800
1000291E  .^ 7C ED         JL SHORT system_6.1000290D
10002920
10002927  .  8B2D 0031001  MOV EBP,DWORD PTR DS:[<&WS2_32.#19>]      WS2_32.send
1000292D  >  6A 00         PUSH 0
1000292F  .  8D443C 18     LEA EAX,DWORD PTR SS:[ESP+EDI+18]
10002933  .  56            PUSH ESI
1000291      50            PUSH EAX
10002        53            PUSH EBX
10002        FFD5          CALL EBP
10002        83F8 FF       CMP EAX,-1
10002     v  74 12         JE SHORT system_6.1000294F
10002        2BF0          SUB ESI,EAX
10002        03F8          ADD EDI,EAX
10002        85F6          TEST ESI,ESI
10002     ^  7F E8         JG SHORT system_6.1000292D
10002        5F            POP EDI
10002        5E            POP ESI
10002        5D            POP EBP
10002        B8 01000000   MOV EAX,1
             5B            POP EBX
             C3            RETN
             5F            POP EDI
             5E            POP ESI
1000      .  5D            POP EBP
100029    .  33C0          XOR EAX,EAX
1000295   .  5B            POP EBX
10002955  .  C3            RETN

Jump is taken
1000290D=system_6.1000290D
```

```
Address   Hex dump                                         ASCII
0006E3E8  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E3F8  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E408  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E418  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E428  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E438  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E448  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E458  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E468  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02  ☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
0006E478  02 02 02 02 02 02 02 02 00 00 00 00 00 00 00 00  ☻☻☻☻☻☻☻☻........
0006E488  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E498  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E4A8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E4B8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E4C8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E4D8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E4E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E4F8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E508  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E518  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E528  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E538  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0006E548  14 01 00 00 05 00 00 00 01 00 00 00 28 0A 00 00  ¶☺..♣...☺...(...
0006E558  02 00 00 00 53 00 65 00 72 00 76 00 69 00 63 00  ☻...S.e.r.v.i.c.
0006E568  65 00 20 00 50 00 61 00 63 00 6B 00 20 00 33 00  e. .P.a.c.k. .3.
```

```
0006E2EC  0006EB08
0006E2F0  0006F8A8
0006E2F4  0006F8C4
0006E2F8  10002D31  syste
0006E2FC  10001636  RETUR
0006E300  00000001
0006E304  00000000
0006E308  02430249
0006E30C  024E0250
0006E310  022F0246
0006E314  024B0255
0006E318  025A024C
0006E31C  02020252
0006E320  02020202
0006E324  02020202
0006E328  02020202
0006E32C  02020202
0006E330  02020202
0006E334  02020202
0006E338  02020202
0006E33C  02020202
0006E340  02020202
0006E344  02020202
0006E348  02020202
0006E34C  02020202
0006E350  02020202
0006E354  02020202
```

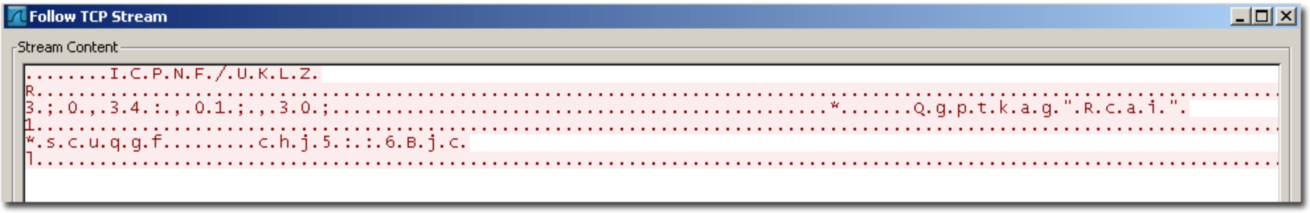
*Figure 6. RAT's encryption algorithm before sending data to its C&C server*



```
10001C93  .    85C0          TEST EAX,EAX
10001C95  .v   0F84 3D01000  JE htrn.10001DD8
10001C9B  .    6A 00         PUSH 0                          ┌Flags = 0
10001C9D  .    8D8424 20010  LEA EAX,DWORD PTR SS:[ESP+120]  │
10001CA4  .    68 08080000   PUSH 808                        │BufSize = 808 (2056.)
10001CA9  .    50            PUSH EAX                        │Buffer
10001CAA  .    53            PUSH EBX                        │Socket
10001CAB  .    FF15 FC30001  CALL DWORD PTR DS:[<&WS2_32.#16>] └recv
10001CB1  .    85C0          TEST EAX,EAX
10001CB3  .v   0F8E 1601000  JLE htrn.10001DCF
10001CB9  .    33C0          XOR EAX,EAX
10001CBB  >   ┌8A8C04 24010  MOV CL,BYTE PTR SS:[ESP+EAX+124]
10001CC2  .   │80F1 02       XOR CL,2
10001CC5  .   │888C04 24010  MOV BYTE PTR SS:[ESP+EAX+124],CL
10001CCC  .   │40            INC EAX
10001CCD  .   │3D 00080000   CMP EAX,800
10001CD2  .^  └7C E7         JL SHORT htrn.10001CBB
```

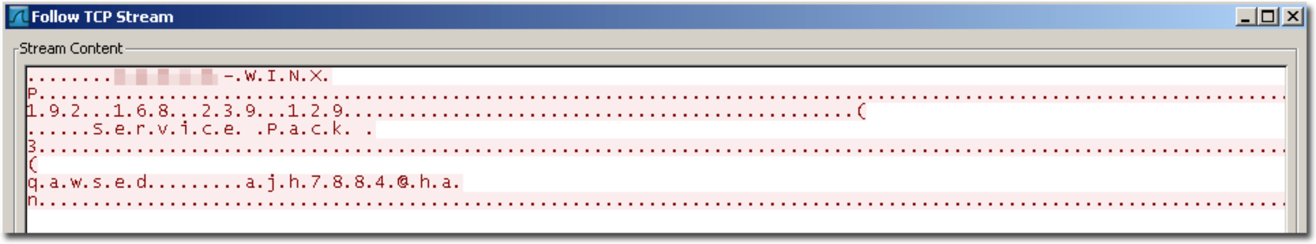
*Figure 7. RAT's decryption code upon receiving data from the C&C server*

During the RAT's phone home, the following TCP traffic is observed on the network:



```
........I.C.P.N.F./.U.K.L.Z.
R..........................................................................................................
3.;.0.,.3.4.:.,.0.1.;.,.3.0.;.......................................*......Q.g.p.t.k.a.g.".R.c.a.i.".
1..........................................................................................................
*.s.c.u.q.g.f........c.h.j.5.:.:.6.B.j.c.
]..........................................................................................................
```

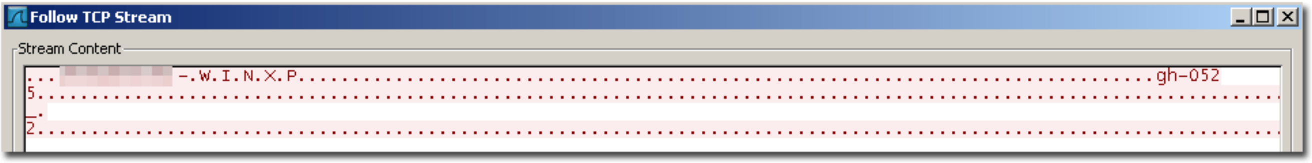
When decrypted, the above traffic looks as follows:



```
........[redacted] -.W.I.N.X.
P..........................................................................................................
1.9.2...1.6.8...2.3.9...1.2.9...........................................(
......S.e.r.v.i.c.e. .P.a.c.k. .
3..........................................................................................................
(
q.a.w.s.e.d.........a.j.h.7.8.8.4.@.h.a.
n..........................................................................................................
```

The majority of the RAT variants used *port 80*. Recent variants, however, were observed to use *port 443*. Other ports we have seen being utilized are *port 5600* and *port 8080*.

Earlier RAT variants did not use encryption on their C&C communication. Moreover, they only sent the computer name and campaign code during phone home. Below is a screenshot of the unencrypted C&C communication.



```
...[redacted] -.W.I.N.X.P.....................................................................gh-052
5..........................................................................................................
_.
2..........................................................................................................
```

The C&C traffic size also varied in previous versions. Some early variants used traffic that are 28H (40 bytes) and 1004H (4,100 bytes) in size.

Additionally, the port, C&C address, campaign code and password are hardcoded in the RAT's malware body in plain text. In some RAT versions, however, they are encrypted and are decrypted only during run-time, possibly to protect the RAT from static analysis by security researchers.

These variations in their RAT component indicate that it has since been undergoing development.

## Command and Control

The HeartBeat campaign's C&C domains appear to utilize a site redirection service. Their C&C sites redirect to IP addresses from ISPs in Armenia, USA, Japan, India and Korea. We observed that they updated the IP address of some of their C&C domains. Likewise, all of their IP addresses belong to legitimate ISPs. Considering this, we suspect that these IP addresses are compromised hosts that act as proxy servers which redirects traffic to the actual C&C servers. Again, this adds another layer of anonymity to the HeartBeat perpetrators.

| Domain | IP Address |
|---|---|
| *ahnlab.myfw.us* | *XXX.XXX.217.123 /XXX.XX.121.84* |
| *kissyou01.myfw.us* | *XX.XXX.203.122 / XX.XXX.20.103* |
| *kita.myfw.us* | *XXX.XXX.217.123 / XXX.XX.121.84* |
| *login.sbs.com.PassAs.us* | *XXX.XXX.178.50* |
| *mail2.myfw.us* | *XX.XXX.15.63 / XXX.XXX.198.93* |
| *park007.myfw.us* | *unknown* |
| *snrp.UglyAs.com* | *XXX.XXX.169.45* |
| *www.banking.com.PassAs.us* | *XXX.XXX.178.50* |
| *www.huyang.go.kr.PassAs.us* | *XXX.XXX.217.123 / XX.XXX.136.115* |
| *www.kinu.or.kr.rr.nu* | *XXX.XXX.178.50* |
| *www.kndu.ac.kr.myfw.us* | *XXX.XXX.4.180* |
| *young03.myfw.us* | *XX.XXX.203.122* |

*Table 1. List of HeartBeat C&Cs*

## HeartBeat Campaign Codes and Decoy Documents

The campaign codes and decoy documents used by the HeartBeat attackers provided valuable insights on their campaigns. In fact, majority of their campaign codes included number combinations which represented the month and date in MMDD format when the attack attempt was executed. The rest of the campaign code string often describes the decoy document that was used in a specific campaign. For instance, a campaign code from October 2011 is "army-1022" where attackers used a decoy document containing military-related information.

| Campaign code | Password |
|---|---|
| 1119HWP | *None* |
| kris0315 | *None* |
| PDF-0417 | *None* |
| gh-0525 | *None* |
| 0909-jpg | qawsed |
| 0916 | qawsed |
| jpg-jf-0925 | qawsed |
| army-1022 | qawsed |
| 1103-ghui | qawsed |
| 1113-minzhu | qawsed |
| ajh7884@han | qawsed |
| 001 | qawsed |
| 0305-ziyoudang | qawsed |
| 0326-xuehui | qawsed |
| 0328-junf | qawsed |
| 0329-mnd | qawsed |
| 1q2w3e4r | *None* |
| 0520-tiegang | qawsed |
| guohui-0604 | qawsed |

*Table 2. Campaign codes used*

On the other hand, decoy documents' contents were also very specific to their targets. For example, some of these documents included logos of specific groups. This information helped us identify their targeted organizations and communities in their previous campaigns.

# Relationships among C&C Domains, IPs, and Campaigns

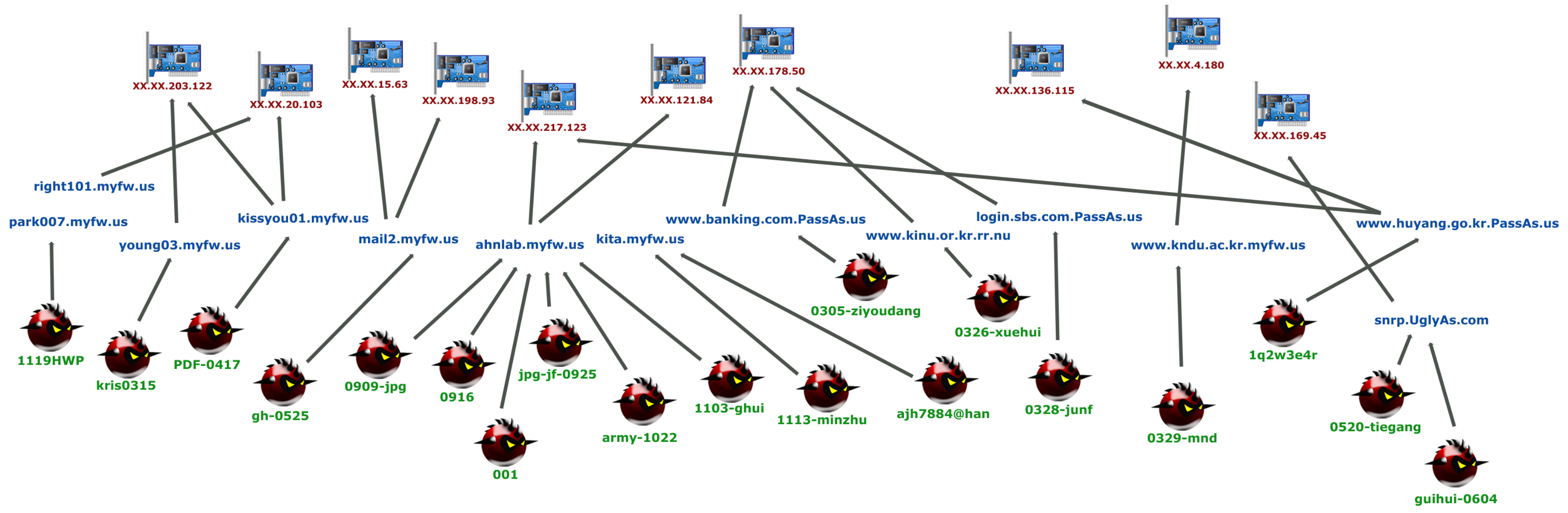


*Figure 7. Relationships between HeartBeat attack components*

## Attribution

Clues relating to the attackers remain very limited. Using compromised hosts as C&C proxy servers minimizes the possibility of tracking potential threat actors. While a number of their campaign codes included Chinese words such as guohui, xuehui and minzhu, they appear to be comfortable using the English language. Some of the C&C domain names even contained English words. In addition, the binder tool and the RAT component are written in English. For instance, some text from the packaged components' body included *"Select Files!"* and *"Bind Success!"*, while the RAT component included strings such as *"Uninstall...ok"* and the name of the RAT itself, *"HeartBeat."*

Threat actors and entities that use collected information from targets may be two separate parties that are only related in a professional and malicious manner. In this case, determining the latter may be impossible. Likewise, it is very difficult to identify the threat actors behind the HeartBeat campaign given the limited amount of information available.

## Conclusion

The Heartbeat campaign has been successfully executing targeted attacks since 2009. In order for attackers to properly track their campaigns and victims, they used campaign codes that contained the campaign dates and strings that described specific campaigns. These campaign codes are embedded in their RAT binaries and were sent to their C&C servers along with information regarding the targets' system. Additionally, they used a commercial site redirection service for their C&C domains. These domains redirected to various IP addresses that belonged to legitimate ISPs, which may be compromised hosts that act as proxy servers. This effectively hides the real location of the attackers behind HeartBeat. While having an isolated target may have helped them stay under the security industry's radar, the attackers illustrated that they were very careful but persistent.

Understanding targeted campaigns and their methodologies is fundamental in protecting both end users and organizations. Not only does it help in coming up with effective defensive strategies through multiple protection layers, it also helps with predicting possible targets in the future and ultimately, raise awareness. As of this writing, the HeartBeat APT campaign remains an active targeted campaign.

## Timeline

We collected 19 set of samples related to HeartBeat campaign from November 2009 to June 2012. This translates to 19 campaigns where the vast majority of which were distributed between 2011 and 2012. Nonetheless, the limited number of samples we were able to obtain still means that the campaign is indeed persistent. The isolated nature of this targeted attack and its small user base may only require the HeartBeat perpetrators to carry out minimal campaigns in order to infiltrate their targets.

| Campaign Date (MM/DD/YY) | MD5 (.DLL component) | Compile Date (MM/DD/YY) |
|---|---|---|
| 11/19/09 | 7c6b44d8d87898e7e5deeeb1961b5ae6 | 9/17/2009 |
| 03/15/11 | fcf42cadb3a932989c8e2b29cef68861 | 12/24/2010 |
| 04/17/11 | aab129ffd3bf5ceeae2e0f332217bebc | 3/18/2011 |
| 05/25/11 | 86547d674e7c7da55e8cae359819832f | 5/6/2011 |
| 09/09/111 | f947e63b14853a69b8ed2648869b5e10 | 7/25/2011 |
| 09/16/11 | 7f1a633384ec97fae9d95d1df9e1135a | 7/25/2011 |
| 09/25/11 | 8816c5be1305488019769c81259dad2a | 9/21/2011 |
| 10/22/11 | 874025a66c2b9d9831c03d1bc114876a | 10/17/2011 |
| 11/03/11 | 4046dec1aa0eebb01fe7469184a95398 | 10/31/2011 |
| 11/13/11 | ba370b17dc9eb1d1e1c3187f0768064f | 10/31/2011 |
| 12/2011 | 51274cefb01cee981a09db83c984213d | 11/28/2011 |
| 02/2012 | d1a2253361045f91ed1902e9ffe2cec3 | 7/18/2011 |
| 03/05/12 | 20bb652e1d2679ed230102aa9676eca0 | 3/1/2012 |
| 03/26/12 | c5c0fea23138cddab96fe22b657f9132 | 3/8/2012 |
| 03/28/12 | ef2bc66ea69327d11d1859af26f5aef9 | 3/8/2012 |
| 03/29/12 | 8e50af054d2c0b45c88082d53c4fc423 | 3/8/2012 |
| 04/2012 | b1e47ecd68c1c151866cec275716aa67 | 4/18/2012 |
| 05/20/12 | 6d205e78fb7730066c116b0c2dffa398 | 5/2/2012 |
| 06/04/12 | 5ec175512ba3c6e78597af48bbe6ca60 | 5/2/2012 |

*Table 3. Specific dates of HeartBeat campaigns*

We did not obtain a campaign sample from 2010. However, we highly suspect that their operation was also active during that year. In fact, we can see in the second MD5 above that the sample was compiled in December 24, 2010. Also, it is possible that some of the campaign's attacks may not have been escalated to antivirus firms by infected users, or simply remains undiscovered.

## Defending against the HeartBeat Campaign

Essential components of defense against the HeartBeat campaign are security-related policies within enterprises. Once an attack is identified, a good cleanup strategy should focus on determining the attack vector and cutting off communications with the C&C server. It is also vital to determine the scope of the compromise and assessing the damage through data analysis and forensics.

The following best practices are also advised:

- Disable services that are related to the HeartBeat RAT component.
- Enable system's firewall
- Keep software and operating systems updated with latest patches released by vendors to address vulnerabilities and exploits.
- Block unused ports to disallow malware from using these ports to communicate and/or enforce commands.
- Monitor network connections for any suspicious connection or connectivity.
- Regularly update list of sites that are trusted.
- Configure your email server to block or remove email that contain file attachments using extensions such as .VBS, .BAT, .EXE, .PIF and .SCR files.
- Avoid opening email attachments and clicking embedded links from unknown sources
- Block any file with more than one file type extension.
- When a computer is compromised, isolate it immediately from the network.
- Configure your system to show hidden files and folders and display file extensions.
- Don't save login credentials on the local computer.

## Trend Micro Threat Protection Against The HeartBeat Campaign Components

The following table summarizes the Trend Micro solutions for the components of the HeartBeat campaign. Trend Micro recommends a comprehensive security risk management strategy that goes further than advanced protection to meet the real-time threat management requirements of dealing with targeted attacks.

| Attack Component | Protection Technology | Trend Micro Solution |
|---|---|---|
| HeartBeat TCP communication is blocked in the network layer as `TCP_HBEAT_REQUEST` | Web Reputation | Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)*<br>Server *(Deep Security)*<br>Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)*<br>Network *(Deep Discovery)*<br>Gateway *(InterScan Web Security, InterScan Messaging Security)*<br>Mobile *(Mobile Security)* |
| TROJ_DRPBEAT and BKDR_HBEAT variants | File Reputation (Antivirus/Anti-malware) | Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)*<br>Server *(Deep Security)*<br>Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)*<br>Network *(Deep Discovery)*<br>Gateway *(InterScan Web Security, InterScan Messaging Security)*<br>Mobile *(Mobile Security)* |
| *XXX.XXX.217.123*<br>*XXX.XX.121.84*<br>*XX.XXX.203.122*<br>*XX.XXX.20.103*<br>*XXX.XXX.217.123*<br>*XXX.XX.121.84*<br>*XXX.XXX.178.50*<br>*XX.XXX.15.63*<br>*XXX.XXX.198.93*<br>*XXX.XXX.169.45*<br>*XXX.XXX.178.50*<br>*XXX.XXX.217.123*<br>*XX.XXX.136.115*<br>*XXX.XXX.178.50*<br>*XXX.XXX.4.180*<br>*XX.XXX.203.122*<br>*ahnlab.myfw.us*<br>*kissyou01.myfw.us*<br>*kita.myfw.us*<br>*login.sbs.com.PassAs.us*<br>*mail2.myfw.us*<br>*park007.myfw.us*<br>*snrp.UglyAs.com*<br>*www.banking.com.PassAs.us*<br>*www.huyang.go.kr.PassAs.us*<br>*www.kinu.or.kr.rr.nu*<br>*www.kndu.ac.kr.myfw.us*<br>*young03.myfw.us* | Web, Domain, and IP Reputation | Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)*<br>Server *(Deep Security)*<br>Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)*<br>Network *(Deep Discovery)*<br>Gateway *(InterScan Web Security, InterScan Messaging Security)*<br>Mobile *(Mobile Security)* |

December 2012 | APT Campaign Quick Profile: HEARTBEAT

Advanced persistent threats (APTs) refer to a category of threats that aggressively pursue and compromise specific targets to maintain persistent presence within the victim's network so they can move laterally and exfiltrate data. Unlike indiscriminate cybercrime attacks, spam, web threats, and the like, APTs are much harder to detect because of the targeted nature of related components and techniques. Also, while cybercrime focuses on stealing credit card and banking information to gain profit, APTs are better thought of as cyber espionage.

# HEARTBEAT

cout@@3 stream_withassign@@
"HeartBeat Fail ReConnect... OK!"

## First Seen

**Individual targeted attacks are not one-off attempts. Attackers continually try to get inside the target's network.**

The "HeartBeat" campaign has been persistently pursuing government agencies since 2009. The samples collected related to this campaign covered attacks seen from November 2009 to June 2012, although majority of the attacks were seen in 2011 and 2012.

## Victims and Targets

**APT campaigns target specific industries or communities of interest in specific regions.**

The HeartBeat campaign targets South Korean government organizations and institutions like political parties, media outfits, a national policy research institute, a military branch of South Korean armed forces, a small business sector organization, and branches of the South Korean government.

## Operations

**The 1st-stage computer intrusions often use social engineering. Attackers custom-fit attacks to their targets.**

The threat actors behind HeartBeat install a RAT in system. The RAT arrives as a disguised or fake document which is actually a bundled file. The bundled file contains both a decoy document and the RAT installer that has been packaged together using a binder tool. The campaign's decoy documents used the file formats .JPG, .PDF, XLS, and HWP, the Korean government standard word processor format.

## Possible Indicators of Compromise

**Attackers want to remain undetected as long as possible. A key characteristic of these attacks is stealth.**

The following indicators suggest an infection by the HeartBeat campaign: contiguous 02H bytes communication in the network, the presence of certain files and registries as detailed in the paper, and network connections to certain IPs and domains, including the presence of files detected as **TROJ_DRPBEAT and BKDR_HBEAT**.

## Relationship with other APT Campaigns

This attack does not seem to have any relationship with other APT campaigns.

## TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

## TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

**U.S. toll free:** 1 +800.228.5651
**Phone:** 1 +408.257.1500
**Fax:** 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud