# Bisonal Malware Used in Attacks Against Russia and South Korea

By Kaoru Hayashi, Vicky Ray

Published: 2018-07-31 · Archived: 2026-04-05 15:05:44 UTC

Summary
In early May, Unit 42 discovered an attack campaign against at least one defense company in Russia and one unidentified organization in South Korea delivering a variant of Bisonal malware. While not previously publicly documented, the variant has been in the wild since at least 2014. There are three primary differences between it and older Bisonal malware including a different cipher and encryption for C2 communication, and a large rewrite of the code for both network communication and maintaining persistence. To date, we have only collected 14 samples of this variant, indicating it may be sparingly used. The adversary behind these attacks lured the targets into launching the Microsoft Windows executable malware by masquerading it as a PDF file (using a fake PDF icon) and reusing publicly available data for the decoy PDF file's contents.
Attacks using Bisonal have been blogged about in the past. In 2013, both COSEINC and FireEye revealed attacks using Bisonal against Japanese organizations . In October 2017, AhnLab published a report called "Operation Bitter Biscuit," an attack campaign against South Korea, Japan, India and Russia using Bisonal and its successors, Bioazih and Dexbia. We believe it is likely these tools are being used by one group of attackers.
Though Bisonal malware has been in the wild for at least seven years and frequently updated, the actors keep using same high-level playbooks. Common features of attacks involving Bisonal include:

- Usually targeting organizations related to government, military or defense industries in South Korea, Russia, and Japan.
- In some cases, the use of Dynamic DNS (DDNS) for C2 servers.
- The use of a target or campaign code with its C2 to track victim or attack campaign connections.
- Disguising the Bisonal malware as a PDF, Microsoft Office Document or Excel file.
- The use of a decoy file in addition to the malicious PE file
- In some cases, code to handle Cyrillic characters on Russian-language operating systems.

We observed all these characteristics in the latest attacks against both Russia and South Korea.

## Targeting Russia

While investigating attack campaigns, Unit 42 discovered a targeted attack against at least one organization in Russia which provides communication security services and products. The targeted organization specialises in encryption and cryptographic services and develops a broad number of secure communication products which also includes telecommunication systems and data protection facilities. Given the sensitivity of the products being developed by the target organization, it is not a surprise to see a targeted attack towards the organisation by a known threat actor.
Figure 1 shows the spear-phishing email sent to the target organization. The email was spoofed to look like it was sent from Rostec, a Russian state corporation that promotes the development, production and export of high-tech industrial products. The contents of the email suggest it was sent from the legal support and corporate governance department of Rostec and includes project details aimed at improving the housing conditions of defence industry workers. It is interesting to note there is a relationship between the target company and Rostec: the attackers may be trying to exploit the relationship between Rostec and the target to add an additional air of legitimacy to the attack.

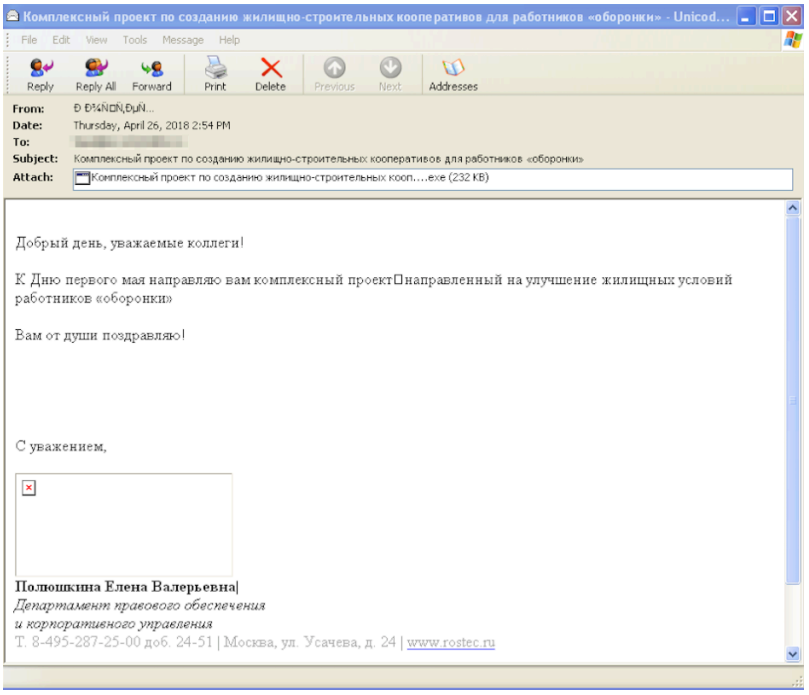



*Figure 1. Spear-phishing email sent to the Russian company*

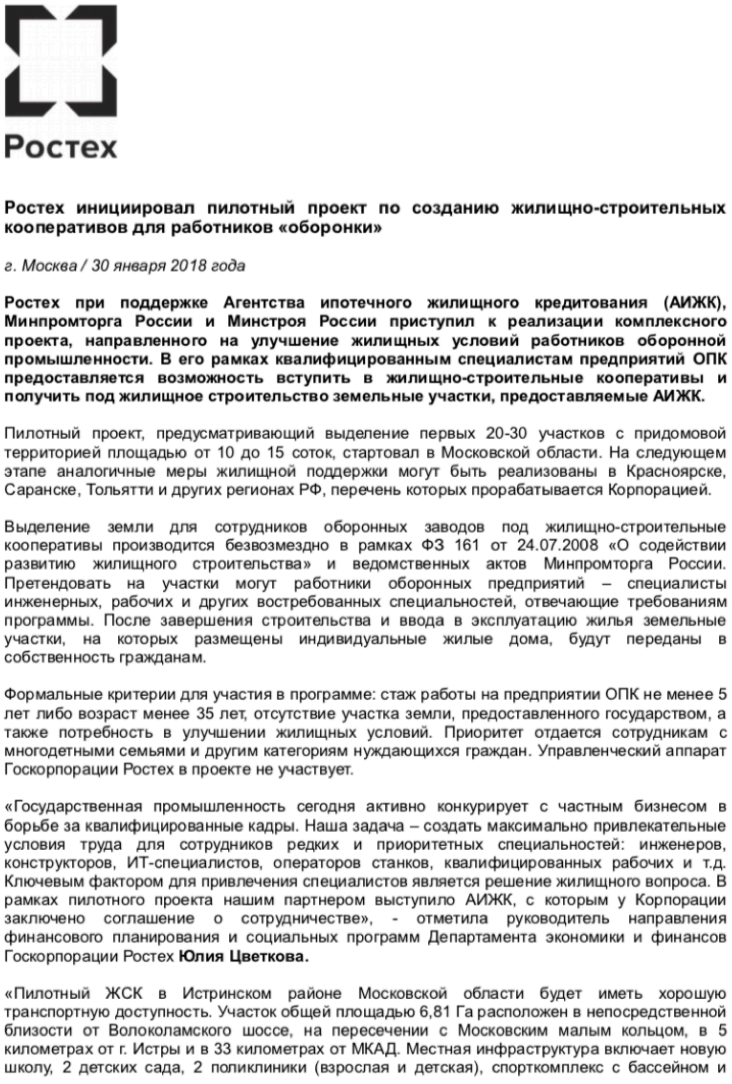
Below is the translation from Russian into English by Google Translate.

*Subject:*
*A comprehensive project to create housing and construction cooperatives for defence workers*

*Body:*
*Good afternoon, dear colleagues!*
*By the May Day, I am sending you a comprehensive project aimed at improving the housing conditions of defence industry workers*
*Congratulations!*

*Attachment:*
*Comprehensive project for the creation of housing construction cooperatives for defence workers .exe*

As you can see in Figure 1, some email clients do not display the attachment as the PDF. However, if you save the file on the computer, it looks like a PDF document because the executable file has the PDF icon in the resource.
Once the malicious executable attachment is opened, the main payload is dropped in the victim machine and displays a decoy file to the victim. Figure 2 shows the contents of the decoy file which is a PDF whose contents are an exact match to an article published on Rostec's website on January 30th, 2018. The article discusses new housing project plans by Rostec and other state departments, and the benefits to the defence industry workers who are eligible for free housing under the project.



Ростех

**Ростех инициировал пилотный проект по созданию жилищно-строительных кооперативов для работников «оборонки»**

*г. Москва / 30 января 2018 года*

**Ростех при поддержке Агентства ипотечного жилищного кредитования (АИЖК), Минпромторга России и Минстроя России приступил к реализации комплексного проекта, направленного на улучшение жилищных условий работников оборонной промышленности. В его рамках квалифицированным специалистам предприятий ОПК предоставляется возможность вступить в жилищно-строительные кооперативы и получить под жилищное строительство земельные участки, предоставляемые АИЖК.**

Пилотный проект, предусматривающий выделение первых 20-30 участков с придомовой территорией площадью от 10 до 15 соток, стартовал в Московской области. На следующем этапе аналогичные меры жилищной поддержки могут быть реализованы в Красноярске, Саранске, Тольятти и других регионах РФ, перечень которых прорабатывается Корпорацией.

Выделение земли для сотрудников оборонных заводов под жилищно-строительные кооперативы производится безвозмездно в рамках ФЗ 161 от 24.07.2008 «О содействии развитию жилищного строительства» и ведомственных актов Минпромторга России. Претендовать на участки могут работники оборонных предприятий – специалисты инженерных, рабочих и других востребованных специальностей, отвечающие требованиям программы. После завершения строительства и ввода в эксплуатацию жилья земельные участки, на которых размещены индивидуальные жилые дома, будут переданы в собственность гражданам.

Формальные критерии для участия в программе: стаж работы на предприятии ОПК не менее 5 лет либо возраст менее 35 лет, отсутствие участка земли, предоставленного государством, а также потребность в улучшении жилищных условий. Приоритет отдается сотрудникам с многодетными семьями и другим категориям нуждающихся граждан. Управленческий аппарат Госкорпорации Ростех в проекте не участвует.

«Государственная промышленность сегодня активно конкурирует с частным бизнесом в борьбе за квалифицированные кадры. Наша задача – создать максимально привлекательные условия труда для сотрудников редких и приоритетных специальностей: инженеров, конструкторов, ИТ-специалистов, операторов станков, квалифицированных рабочих и т.д. Ключевым фактором для привлечения специалистов является решение жилищного вопроса. В рамках пилотного проекта нашим партнером выступило АИЖК, с которым у Корпорации заключено соглашение о сотрудничестве», - отметила руководитель направления финансового планирования и социальных программ Департамента экономики и финансов Госкорпорации Ростех **Юлия Цветкова.**

«Пилотный ЖСК в Истринском районе Московской области будет иметь хорошую транспортную доступность. Участок общей площадью 6,81 Га расположен в непосредственной близости от Волоколамского шоссе, на пересечении с Московским малым кольцом, в 5 километрах от г. Истры и в 33 километрах от МКАД. Местная инфраструктура включает новую школу, 2 детских сада, 2 поликлиники (взрослая и детская), спорткомплекс с бассейном и

*Figure 2 Decoy pdf file*

Upon further analysis of the malware payload, we determined it is part of the Bisonal malware family. Since the details of the malware family have already been published, we will discuss some of the unique indicators and techniques the threat actor behind Bisonal employed in this campaign.

Malware Analysis

**Malware Dropper**

The dropper executable file in the Russian attack hides the encrypted Bisonal DLL file and non-malicious decoy file at the end of its body. Once executed, the dropper decrypts the data blob using the RC4 cipher with the key, “34123412”, saves them in the path shown below and executes them.

| Type | PATH | SHA256 |
|---|---|---|
| Dropper EXE | N/A | b1da7e1963dc09c325ba3ea2442a54afea02929ec26477a1b120ae44368082f8 |
| Bisonal DLL | C:\Windows\Temp\pvcu.dll | 1128D10347DD602ECD3228FAA389ADD11415BF6936E2328101311264547AFA75 |
| Russian Decoy PDF | C:\Windows\Temp\Комплексный проект по созданию жилищно-строительных кооперативов для работников оборонки.pdf | F431E0BED6B4B7FFEF5E40B1B4B7078F2538F2B2DB2869D831DE5D7DF26EE6CD |

*Table 1. File hashes and paths targeting Russia*

The dropper then creates following registry entry to execute the Bisonal sample when the computer reboots:
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Run\"vert" = "rundll32.exe c:\windows\temp\pvcu.dll , Qszdez"

Bisonal main module

The DLL (pvcu.dll) is Bisonal malware but using a different cipher for C2 communication that other publicly documented samples. Booz Allen Hamilton in 2014 and AhnLab in 2015 reported on Bisonal using a simple XOR cipher to hide the C2 address strings in the body. The Bisonal sample we observed in this case employs the RC4 cipher with the key "78563412". To date, all Bisonal samples we have seen using RC4 use this same key. The oldest sample we have dates to 2014, so this variant has been in the wild for several years.

Adding to the change in encryption type, a large part of the code such as network communication procedures, and the persistence method have been re-written. For example, the Bisonal malware in 2012 used send() and recv() APIs to communicate with its C2. For this variant, the developer wholly recreated C2 code from scratch by using other network APIs, such as HttpSendRequest() and InternetReadFile().

This Bisonal variant used in the latest attack communicates with one of the following hard-coded C2 addresses by using the HTTP POST method on TCP port 443.

- kted56erhg.dynssl[.]com
- euiro8966.organiccrap[.]com

These domains are provided by a free DDNS service and both resolve to the same IP address, 116.193.155[.]38.

When this Bisonal variant communicates with its C2, the malware sends an HTTP POST request with the static strings "ks8d" and "akspbu.txt", and the IP address of the compromised machine. Figure 3 shows the initial HTTP POST request to the C2 server.

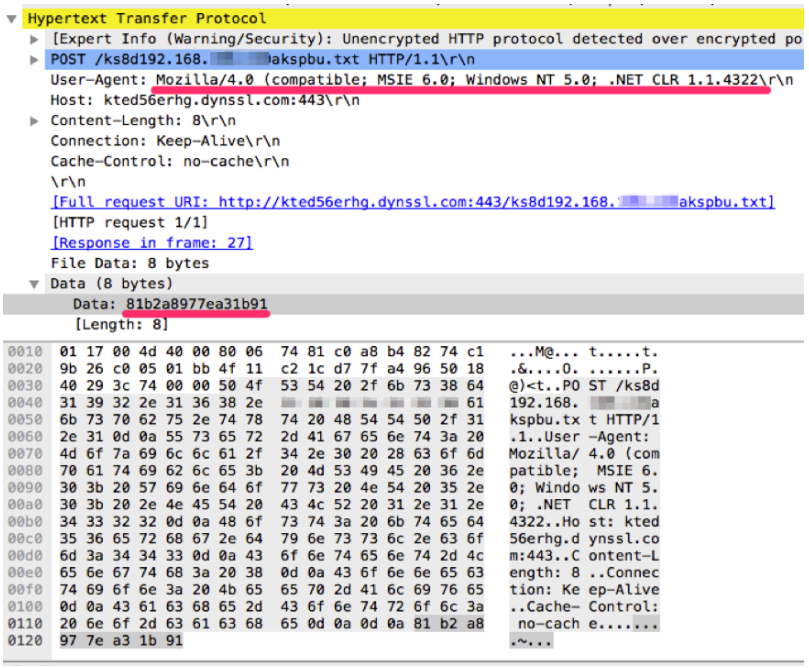



*Figure 3. Initial network C2 beacon*

Readers may notice the missing closing parenthesis in the User Agent request header. That string is hardcoded in this malware variant. We have more than 230 samples of Bisonal in total and only 14 samples since 2014 use this incomplete User Agent string. It is unclear whether the author forgot to add closing parenthesis while developing the code, or intentionally use this string for validating the connection to the C2 server. Either way, it can be a good Indicator in network logs for a possible Bisonal infection.

C2 Communication

Another sign of the infection is the data being sent to the C2 server during the initial connection. Every time this variant of Bisonal communicates with its C2, it sends a unique id number and backdoor command in the first eight bytes. The malware sends hardcoded DWORD values (0x10000 and 0x3E7) just for the initial connection and receives updated values from the C2 and uses them for further communication. As described above, all communications between this Bisonal variant and C2 are encrypted by RC4 cipher with the static key "78563412". As the result of enciphering static values, the backdoor always sends identical eight bytes of data (81b2a8977ea31b91) to the C2 first.

Soon after receiving the initial beacon from the victim infected with Bisonal, the C2 replies with a session id number and backdoor command. The session id number is consistent throughout the C2 communication. The malware then processes the

given command on the compromised system and sends the result back to C2 with the session id number and the backdoor command number. Then the C2 replies with that same session id number. The backdoor waits five seconds and restarts communication with the C2 with the same session id number.

Below is an example of the reply to the command, “get system info”. The actual traffic between the C2 and Bisonal sample is on the left side, and the decrypted payload is on the right side. The first DWORD (four bytes) is the given session id, 0x00000003, and the next DWORD is a backdoor command, 0x000000C8. At offset 8 of the decrypted payload, there is a campaign or target code. In this sample, it is “0425god”.


*Figure 4 Decrypted payload showing the target/campaign code*

Following is the diagram of the session between Bisonal and C2.

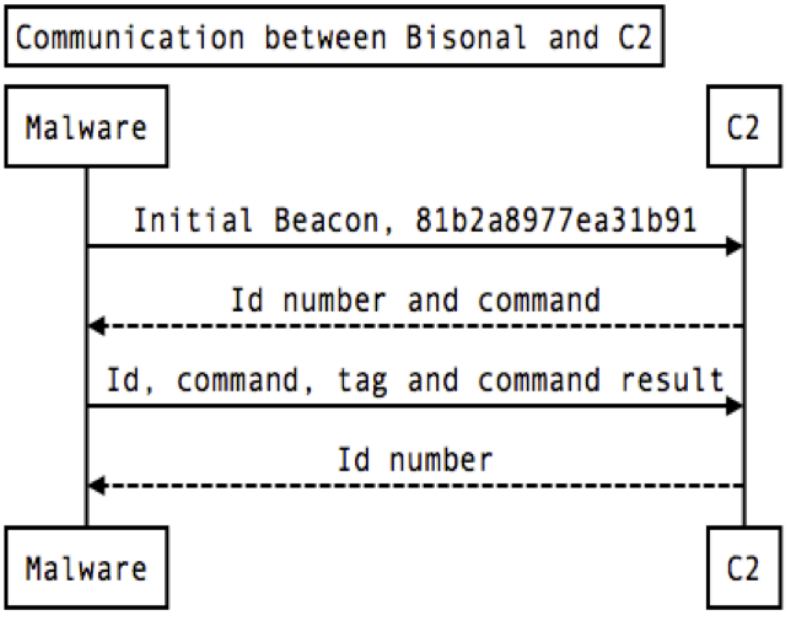



*Figure 5. Bisonal C2 communication flow*

The following table shows the list of backdoor commands this sample supports.

| Command | Meaning |
|---|---|
| 0x000000C8 | gets system info |
| 0x000000C9 | gets running process list |
| 0x000000CA | terminates process |
| 0x000000CB | accesses cmd shell |
| 0x000000CD | downloads file |
| 0x000000CF | executes file |
| 0x000000D1 | creates file |

*Table 2 Backdoor commands*

Strong Interests in Cyrillic

Previous reports have discussed Bisonal malware used in attacks against Japan, South Korea and Russia. This particular sample we found targeted an organization in Russia and there is a specific system language check for Cyrillic and no others. When the backdoor receives the shell access command, it checks the code page of the compromised system. If it's Cyrillic and the command to the shell is not 'ipconfig', the threat converts the command result text encoding from Cyrillic to UTF-16. For any other code page the malware presumes the resulting text as default Windows ANSI code page and also converts it to UTF-16. It is not known why the malware author called out Cyrillic specifically when the malware would convert any text to UTF-16. Windows ANSI code pages supports ASCII characters and non-ASCII values as the international characters depends on the OS language. UTF-16 can support maximum 1 million characters in Unicode. To avoid corrupting Cyrillic (and other language) characters in the results, the developer added the code to the malware.

```
.text:10002071                  cmp     [esp+0A90h+codepage], 866 ; Cyrillic
.text:10002079                  jnz     short cp_is_not_Cyrillic
.text:1000207B                  push    offset aIpconfig ; "ipconfig"
.text:10002080                  push    offset shell_command ; wchar_t *
.text:10002085                  call    _wcscmp
.text:1000208A                  mov     ecx, [esp+0A98h+NumberOfBytesRead]
.text:1000208E                  add     esp, 8
.text:10002091                  lea     edx, [esp+0A90h+WideCharStr]
.text:10002098                  test    eax, eax
.text:1000209A                  push    ecx
.text:1000209B                  push    edx
.text:1000209C                  lea     eax, [esp+0A98h+Buffer]
.text:100020A3                  push    0FFFFFFFFh
.text:100020A5                  push    eax
.text:100020A6                  push    ebx
.text:100020A7                  jz      short command_is_ipconfig
.text:100020A9                  push    866
.text:100020AE                  jmp     short command_is_not_ipconfig
.text:100020B0 ; ---------------------------------------------------------
.text:100020B0
.text:100020B0 cp_is_not_Cyrillic:                      ;
.text:100020B0                  mov     ecx, [esp+0A90h+NumberOfBytesRead]
.text:100020B4                  lea     edx, [esp+0A90h+WideCharStr]
.text:100020BB                  push    ecx             ; cchWideChar
.text:100020BC                  push    edx             ; lpWideCharStr
.text:100020BD                  lea     eax, [esp+0A98h+Buffer]
.text:100020C4                  push    0FFFFFFFFh      ; cbMultiByte
.text:100020C6                  push    eax             ; lpMultiByteStr
.text:100020C7                  push    ebx             ; dwFlags
.text:100020C8
.text:100020C8 command_is_ipconfig:                     ;
.text:100020C8                  push    ebx             ; CodePage
.text:100020C9
.text:100020C9 command_is_not_ipconfig:                 ;
.text:100020C9                  call    ebp ; MultiByteToWideChar
```

*Figure 6. Checking of Cyrillic character set*

This Cyrillic/ipconfig checks in the 'shell access' backdoor command exists in some original Bisonal samples found in 2012. The sample (43459f5117bee7b49f2cee7ce934471e01fb2aa2856f230943460e14e19183a6) contains the marker string "bisonal" which is the origin of the malware name. This is one of the many reasons we strongly believe the latest samples are variants of Bisonal.

```
.data:71004010 aBisonal        db 'bisonal',0
.data:71004018 aUzqqvyzm1spptv db 'uzqqvyzm&&',27h,'1spptvq1~k',0
.data:71004018                                          ; DATA XREF: StartAddress+68↑o
.data:71004018                                          ; StartAddress:loc_71002384↑r ...
```

*Figure 7. 'bisonal' marker string*

Targeting South Korea

While investigating other Bisonal samples we found another dropper submitted to an online malware database on March 6. The original file name was "2018년 해양경찰청 공무원 (7급 9급) (2018.03.05).pdf.exe". This translates to "2018 Korean Coast Guard Government Employee (Grade 7, Grade 9).pdf.exe" in English. Similar to the Bisonal variant targeting the

Russian organization, this sample was also disguised as PDF document.


*Figure 8. Malware disguised as PDF*

The dropper executable installs Bisonal and a decoy file in the paths shown in Table 3, below.

| Type | PATH | SHA256 |
|---|---|---|
| Dropper EXE | N/A | 0641fe04713fbdad272a6f8e9b44631b7554dfd1e1332a8afa767d845a90b3fa |
| Bisonal EXE | %Temp%\[random].tmp | 359835C4A9DBE2D95E483464659744409E877CB6F5D791DAA33FD601A01376FC |
| Korean Decoy PDF | [dropper path]\[same file name without .exe].pdf | B2B764597D097FCB93C5B11CBD864AB1BCB894A2A1E2D2DE1C469880F612431C |

*Table 3, File hashes and system installation paths targeting South Korea*

Though the functionality of the two dropper samples look very similar, the dropper code of this sample is completely different from the Russian targeting sample described above.

- The dropper installs the Bisonal EXE file and decoy PDF file. These files are not encrypted and the offset to the EXE and PDF file in the dropper is appended at the end of the dropper file. In the Russian samples, the offset to these files is hardcoded in the code.
- The file name of the decoy file is based on the dropper file name. The dropper code creates a PDF at the same directory, give the same name with itself to the decoy file, removes .exe and adds .pdf in the code. For example, if the file name is ABCDEFG.pdf.exe, the decoy filename would be pdf.pdf.
- The dropper also creates two VBS scripts in the %Temp% directory with a random 4 digits hexadecimal name. One of them opens the decoy PDF file. The other deletes the dropper and the VBS script itself.

The contents of the decoy PDF is a job descriptions with the South Korean Coast Guard. The original document was a Hangul Word Processor(HWP) file posted on the South Korean Coast Guard website on March 5, 2018. Based on the metadata we found in the PDF, we strongly believe that the attacker converted the HWP to PDF. Figure 8, below, shows metadata added to the decoy file when converting the original file to PDF. The metadata indicates that the file was created with Adobe Distiller 8.00 (Windows) on March 6 by “조영태” (Cho Young Tae in English).
Interestingly, the same creator name is found in the decoy PDF file of another sample of the Bisonal variant (dfa1ad6083aa06b82edfa672925bb78c16d4e8cb2510cbe18ea1cf598e7f2722) submitted to an online malware database in September 2014. This decoy is a contact list of Agriculture, Food, Rural Affairs, Oceans and Fisheries Committee of the National Assembly of the Republic of Korea. According to the metadata, this file is also converted from an HWP document with same tool by same creator. Though we don’t know whether the creator is real or fake information, we can say the attacker has not changed this tool and technique for years.


*Figure 8. Metadata in the decoy file*

Main EXE

The installed EXE file is almost exactly the same as the DLL version of Bisonal variant used against the Russian organization. Following is a brief write-up of the Bisonal EXE's behavior. There are only three differences from the DLL sample; creating a registry entry by itself, the C2 domain and the target or campaign code. The EXE's behavior is discussed below.

- It creates the registry entry, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"mismyou" = %Temp%[random].tmp to achieve persistence. In contrast, the DLL version does not create a registry entry because the dropper of the DLL does.
- It decrypts the C2 domain address by using the RC4 cipher with the same key "78563412".
- It connects to hxxp://games.my-homeip[.]com:443/ks8d[ip address]akspbu.txt by using the HTTP POST method with the same incomplete User Agent string "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322"
- It sends the same initial beacon value of 81b2a8977ea31b91 to the C2 server.
- It uses a different target or campaign code, "pmo".
- It has same backdoor commands, starting with 0x000000C8 in hex.
- It also checks the code page and command in "shell access" and converts text from Cyrillic to UTF-16.

Following table is the summary of the Bisonal samples described in this article.

| Year | Target Country | Campaign or Target Code | SHA256 | Cipher | Bisonal Marker |
|---|---|---|---|---|---|
| 2012 | unidentified | 1031 | 43459f5117bee7b49f2cee7ce934471e01fb2aa2856f230943460e14e19183a6 | XOR | YES |
| 2014 | South Korea | 0919-1 | dfa1ad6083aa06b82edfa672925bb78c16d4e8cb2510cbe18ea1cf598e7f2722 | RC4 | NO |
| 2018 | Russia | 0425god | 1128D10347DD602ECD3228FAA389ADD11415BF6936E2328101311264547AFA75 | RC4 | NO |
| 2018 | South Korea | pmo | 359835C4A9DBE2D95E483464659744409E877CB6F5D791DAA33FD601A01376FC | RC4 | NO |

*Table 4 Summary of the Bisonal samples in this blog*

Conclusion

The attackers behind Bisonal have been active for at least 7 years, and the variant used against the Russian and South Korean targets discussed in this blog in the wild since 2014. Since the attackers frequently rewrite functions from scratch and avoid reusing infrastructures, some samples look very different from original Bisonal malware. However, as we discussed in this blog, the same original piece of code referencing the malware name "bisonal" remains in at least some samples.

We are still investigating the connection between the latest attacks discussed in this blog and the previous Bisonal attacks reported by industry colleagues. The high-level TTPs of the adversary behind these Bisonal samples matches with previous Bisonal activity. The targets are military or defense industry in particular countries, it used DDNS for C2 servers, and

tracked connections from their victims by using target or campaign codes, as well as disguising the malware as document file, and using a dropper to install the malware and decoy file. We currently believe one group is behind these attacks, and we continue to investigate.
Palo Alto Networks customers are protected from this threat by:

- WildFire detects all Bisonal files with malicious verdicts
- AutoFocus customers can track these samples with the Bisonal tag
- Traps blocks all of the files associated with Bisonal

IoC
Dropper SHA256:
B1DA7E1963DC09C325BA3EA2442A54AFEA02929EC26477A1B120AE44368082F8
0641FE04713FBDAD272A6F8E9B44631B7554DFD1E1332A8AFA767D845A90B3FA

**Bisonal SHA256:**
43459F5117BEE7B49F2CEE7CE934471E01FB2AA2856F230943460E14E19183A6
DFA1AD6083AA06B82EDFA672925BB78C16D4E8CB2510CBE18EA1CF598E7F2722
1128D10347DD602ECD3228FAA389ADD11415BF6936E2328101311264547AFA75
359835C4A9DBE2D95E483464659744409E877CB6F5D791DAA33FD601A01376FC

**C2:**
jennifer998.lookin[.]at
196.44.49[.]154
www.hosting.tempors[.]com
kted56erhg.dynssl[.]com
euiro8966.organiccrap[.]com
116.193.155[.]38
games.my-homeip[.]com

---