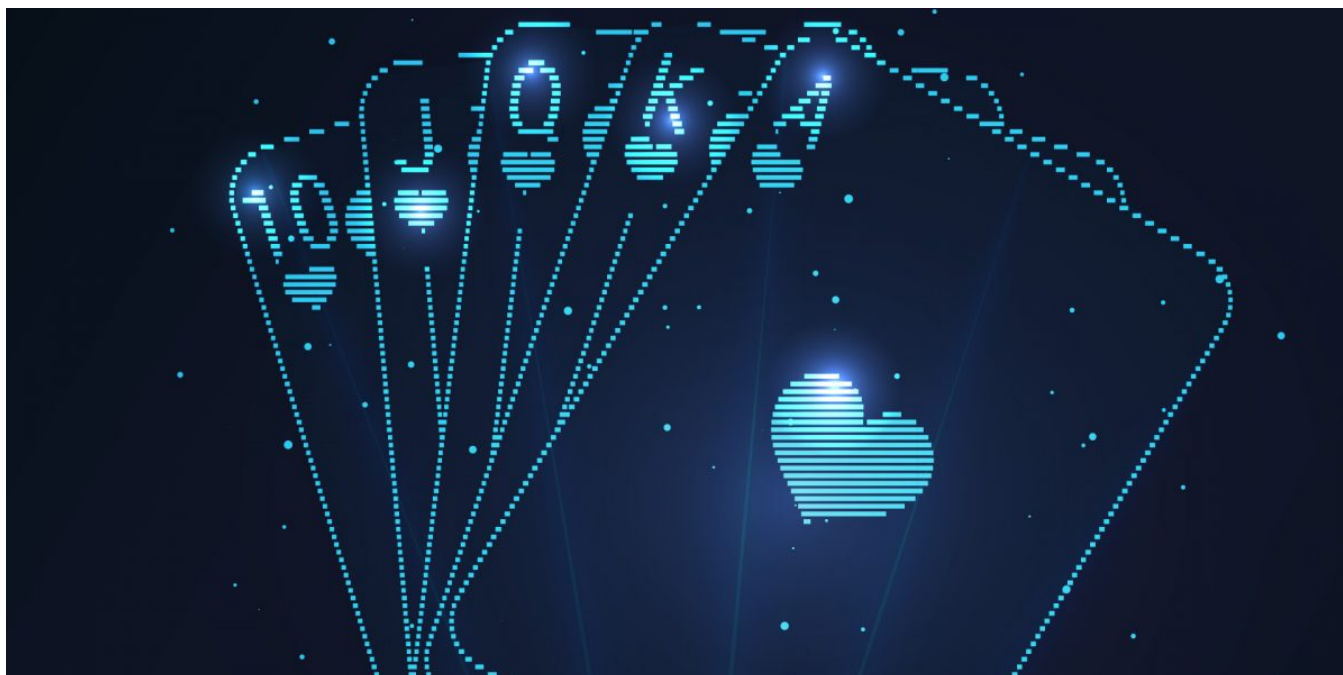


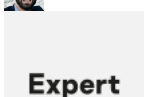


# IAMTheKing and the SlothfulMedia malware family

SL [securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/](https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/)



Authors

-  [Ivan Kwiatkowski](#)
-  [Pierre Delcher](#)
-  **Expert** [Félix Aime](#)

On October 1, 2020, the DHS CISA agency [released information](#) about a malware family called SlothfulMedia, which they attribute to a sophisticated threat actor. We have been tracking this set of activity through our private reporting service, and we would like to provide the community with additional context.

In June 2018, we published the first report on a new cluster of activities that we named IAMTheKing, based on malware strings discovered in a malware sample from an unknown family. Amusingly, other strings present inside of it invited “kupasiky antivirus” to “leave [them] alone”.

```
5:D850h: 6B 69 6C 6C 20 6D 65 20 6F 72 20 6C 6F 76 65 20 kill me or love
5:D860h: 6D 65 00 00 70 6C 65 61 73 65 20 6C 65 61 76 65 me..please leave
5:D870h: 20 6D 65 20 61 6C 6F 6E 65 00 00 00 69 6D 20 74 me alone...im t
5:D880h: 68 65 20 6B 69 6E 67 35 30 34 38 36 33 30 00 00 he king5048630].
5:D890h: 64 6F 6E 74 20 64 69 73 74 75 72 62 20 6D 65 00 dont disturb me.
```

Over time, we identified three different malware families used by this threat actor, one of which was SlothfulMedia. The aim of this blog post is to introduce all of them and to provide data we have been able to gather about the attackers’ interests.

## IAMTheKing’s toolset

### KingOfHearts

This C++ backdoor, which contains the character strings discussed above, is the first element of this toolset we encountered. It comes in EXE or DLL variants, and we have been able to find traces of this family dating back to 2014. We believe it was distributed through spear-phishing e-mails containing malicious Word documents, but have been unable to obtain samples of these. The infection process relies on a PowerShell script that downloads from a remote server a base64-encoded payload hidden in an image file.

In terms of capabilities, KingOfHearts offers nothing more than the basic features you would expect from a backdoor:

- Arbitrary command execution

- File system manipulation: listing drives and files, deleting, uploading and downloading data, etc.
- Listing of running processes with the option to terminate any of them
- Capturing screenshots using a custom standalone utility, described below

Rather than developing sophisticated features, the malware developers instead opted to include anti-debugging and virtualization detection routines. Communications with the C2 server take place over HTTP(S), implemented with the [wsdlpull](#) open source library. The backdoor looks for new orders every second by sending a heartbeat to the C2 (the “HEART” command, hence the name).

We identified two main development branches: one of them sends url-encoded POST data, and the other one sends [JSON objects](#). Both have been used concurrently and otherwise display the same capabilities: we cannot say what motivates attackers to choose the one or the other.

## QueenOfHearts

---

Following our initial discovery, we identified another, more widespread malware family linked to the same threat actor. While it does not contain the anti-analysis countermeasures of its cousin, the rest of its features and overall design decisions map to King of Hearts almost one to one. QueenOfHearts seems to have appeared somewhere in 2017. It is the family designated as PowerPool by our esteemed colleagues from [ESET](#).

QueenOfHearts also interacts with its C2 server over HTTP. It sends simple GET requests containing a backdoor identifier and optional victim machine information, then reads orders located in the cookie header of the reply. Orders come in the form of two-letter codes (e.g.: “xe” to list drives) which tend to vary between samples. As of today, this family is still in active development, and we have observed code refactoring as well as incremental upgrades over 2020. For instance, earlier backdoor responses were sent as base64-encoded payloads in POST requests. They are now compressed beforehand, and additionally supplied through the cookie header.

## QueenOfClubs

---

In the course of our investigations, we discovered another malware strain that appeared to fill the same role as QueenOfHearts. This C++ backdoor also offers similar features as KingOfHearts, as well as the ability to execute arbitrary Powershell scripts. One minute difference is that in this one, screenshot capture capabilities are embedded directly into the program instead of being handled by a separate utility.

It contains a number of links to QueenOfHearts, namely:

- Identical hardcoded file names can be found in both malware strains.
- We observed a number of command and control servers concurrently handling traffic originating from both families.
- QueenOfHearts and QueenOfClubs were on occasion deployed simultaneously on infected machines.

However, it is also our belief that they originate from two separate codebases, although their authors shared common development practices.

The malware designated as SlothfulMedia by US-CERT is an older variant of this family.

## JackOfHearts

---

Astute readers will notice that we did not discuss persistence mechanisms for any of the two aforementioned families. In fact, both of them expect to run in an environment that has already been prepared for them. JackOfHearts is the dropper associated with QueenOfHearts: its role is to write the malware somewhere on the disk (for instance: %AppData%\mediaplayer.exe) and create a Windows service pointing to it as well as a shortcut in the startup folder that is also used to immediately launch QueenOfHearts. This shortcut is the one that contains references to a “david” user highlighted by the DHS CISA report.

Finally, the dropper creates a self-deletion utility in the %TEMP% folder to remove itself from the filesystem.

As of 2020, JackOfHearts is still used to deploy QueenOfHearts.

## Screenshot capture utility

---

A simple program that captures screenshots and saves them as “MyScreen.jpg”. It is sometimes embedded directly inside QueenOfHearts but has also been seen in conjunction with KingOfHearts.

## Powershell backdoor

---

In addition to these malware families, IAmTheKing also leverages an extensive arsenal of Powershell scripts. Recent infection vectors have involved archives sent over e-mail which contain LNK files masquerading as Word documents. Clicking on these links results in the execution of a Powershell backdoor that hides inside custom Windows event logs and retrieves additional scripts over HTTPS, DNS or even POP3S.

The C2 server provides PNG files, which contain additional Powershell scripts hidden through steganography. The code performing this operation comes from the open-source project [Invoke-PSImage](#). This allows operators to stage components on the victim machine, such as:

- An information-stealing utility written in Powershell that collects all documents found on the victim’s machine and sends them in password-protected RAR archives. These archives are sent back to the attackers over e-mail.

- A command execution utility which obtains orders from DNS TXT records. The code to accomplish this is derived from another open-source project, [Nishang](#).
- An information-gathering utility tasked with collecting running processes, disk drives and installed programs with WMI queries. It may also steal passwords saved by the Chrome browser.
- A spreader script that lists computers connected to the domain, and tries to open a share on each of them to copy a binary and create a remote scheduled task.
- A home-made keylogger.
- QueenOfHearts, one of the malware families described above.

## Lateral movement

---

Once the attackers have gained access to a machine through any of the tools described above, they leverage well-known security testing programs to compromise additional machines on the network. In particular, we found evidence of the following actions on the target:

- Microsoft's SysInternals suite: ProcDump to dump the exe process and PsExec to run commands on remote hosts.
- LaZagne and Mimikatz to collect credentials on infected machines.
- Built-in networking utilities such as ipconfig.exe, net.exe and ping.exe, etc. for network discovery.

## Victimology

---

Until very recently, IAmTheKing has focused exclusively on collecting intelligence from high-profile Russian entities. Victims include government bodies and defense contractors, public agencies for development, universities and companies in the energy sector. This threat actor's geographic area of interest is so specific that KingOfHearts, QueenOfHearts and even recent versions of JackOfHearts include code referring specifically to the Russian language character set:

```

BOOL is_system()
{
    BOOL result; // eax
    DWORD buffer_size; // [esp+28h] [ebp-2Ch] BYREF
    char *v2; // [esp+2Ch] [ebp-28h]
    CHAR username[32]; // [esp+30h] [ebp-24h] BYREF

    v2 = "SYSTEM";
    username[0] = 0;
    *(_DWORD *)&username[1] = 0;
    *(_DWORD *)&username[5] = 0;
    *(_DWORD *)&username[9] = 0;
    *(_DWORD *)&username[13] = 0;
    *(_DWORD *)&username[17] = 0;
    *(_DWORD *)&username[21] = 0;
    *(_DWORD *)&username[25] = 0;
    *(_WORD *)&username[29] = 0;
    username[31] = 0;
    buffer_size = 32;
    GetUserNameA(username, &buffer_size);
    if ( GetSystemDefaultUILanguage() == 1049 ) // Russian - Russia
        result = strncmp(username, "нєñòàìà", strlen("нєñòàìà")) == 0;
    else
        result = strncmp(username, v2, strlen(v2)) == 0;
    return result;
}

```

In 2020, we discovered rare incidents involving IAmTheKing in central Asian and Eastern European countries. The DHS CISA also reports activity in Ukraine and Malaysia. Our data however indicates that Russia overwhelmingly remains IAmTheKing's primary area of operation.

There is currently debate within our team on whether this constitutes a slight shift in this threat actor's targeting, or if its toolset is now shared with other groups. We are unable to provide a definitive answer to this question at this juncture.

## Conclusion

---

While the public has only recently discovered this set of activity, IAmTheKing has been very active for a few years. Considering the type of organizations that cybercriminals have been targeting, we felt that there was little public interest in raising awareness about this group beyond our trusted circle of industry partners. However, now that researchers have started investigating this threat actor, we want to assist the community as much as possible by providing this brief summary of our knowledge of IAmTheKing.

Based on the type of information IAmTheKing is after, we believe that it is state-sponsored. Its toolset is rapidly evolving, and it is not afraid to experiment with non-standard communications channels. The group is characterized by a mastery of traditional pentesting methodologies and a solid command of Powershell. Data available to us indicates that it has achieved operational success on numerous occasions.

Kaspersky will keep investigating incidents related to this group in the foreseeable future and has gathered a detailed view of their 2020 activity so far. We invite individuals or companies who think they might be – or have been – targeted by IAmTheKing to get in touch with us for additional information, or otherwise request access to our Threat Intelligence Portal for regular updates on this threat actor.

## YARA rules

---

In virtually all our investigations, we write YARA rules to hunt for additional malware samples and get a better idea of each family's prevalence. In the spirit of sharing knowledge with the community and assisting research efforts on this threat actor, we are happy to release a few of these rules, which will allow defenders to identify recent samples from the families described above. If you are unfamiliar with YARA or would like to learn more about the art of writing rules, please check out the [online training](#) written by members of GREAT.

```
1 rule apt_IAmTheKing_KingOfHearts {
2   meta:
3     description = "Matches IAmTheKing's KingOfHearts C++ implant"
4     author = "Kaspersky Lab"
5     copyright = "Kaspersky Lab"
6     version = "1.0"
7     type = "APT"
8     filetype = "PE"
9     last_modified = "2020-01-20"
10  strings:
11    $payload_fmt = "cookie=%s;type=%s;length=%s;realdata=%send" ascii
12    $cmd1 = "HEART" ascii
13    $cmd2 = "CMDINFO" ascii
14    $cmd3 = "PROCESSINFO" ascii
15    $cmd4 = "LISTDRIVE" ascii
16    $cmd5 = "LISTFILE" ascii
17    $cmd6 = "DOWNLOAD" ascii
18  condition:
19    uint16(0) == 0x5A4D and filesize < 1MB and
20    ($payload_fmt or all of ($cmd*))
21 }
22
23 rule apt_IAmTheKing_KingOfHearts_json {
24   meta:
25
26     description = "Matches IAmTheKing's KingOfHearts JSON C++ implant"
27     author = "Kaspersky Lab"
28     copyright = "Kaspersky Lab"
29     version = "1.0"
30     type = "APT"
31     filetype = "PE"
32     last_modified = "2020-01-20"
33  strings:
34    $user_agent = "Mozilla/4.0 (compatible; )" ascii
35    $error = "write info fail!!! GetLastError-->%u" ascii
36    $multipart = "Content-Type: multipart/form-data; boundary=--MULTI-PARTS-FORM-DATA-BOUNDARY\x0D\x0A" ascii
37  condition:
38    uint16(0) == 0x5A4D and filesize < 1MB and all of them
```

```

39 }
40
41 rule apt_IAmTheKing_QueenOfHearts_2020 {
42   meta:
43     author = "Kaspersky"
44     copyright = "Kaspersky"
45     version = "1.0"
46     type = "APT"
47     filetype = "PE"
48     description = "Find IAmTheKing's QueenOfHearts 2020 variants"
49     last_modified = "2020-09-29"
50   strings:
51     $s1 = "www.yahoo.com" fullword wide
52     $s2 =
53 "8AAAAHicJY9HDslwFAXnMmQHIsGULKKIUPZwA0SNqCEIcXwGI+vL781vdknNjR17PvQ48eLKhZKGlSJMwoE7T2nBipSKNQtpy0PSISSqf
54   ascii
55     $s3 =
56 "2gAAAAHicHYy7DoJAEEXp2xMKJVEehoKSwsLSqMLCRh5BDTK33vWTHbuzpk7NzLQEMiJ9pmJDy0LK536tA7q1xfYcVJf7Km96jz5yGJs
57   ascii
58     $s4 =
59 "2gAAAAHicHY/JDoJAEAXrZ+SmEUSUAYeueNc/MOBCVfwwxs+3nEw6/V71ilp6Wg48GXEmTc3rpQ86SmsRBy585IWbllZsqOS9jwkQ0mke
60   ascii
61     $s5 = "MyScreen.jpg" fullword wide
62     $s6 = "begin mainthread" fullword wide
63     $s7 = "begin mainthread ok" fullword wide
64     $s8 = "getcommand error" fullword wide
65     $s9 = "querycode error" fullword wide
66     $s10 = "{session:[{'name':'admin_001','id':21,'time':12836123}],jpg:" fullword ascii
67     $s11 = "cookie size :%d" fullword wide
68     $s12 = "send request error:%d" fullword wide
69     $s13 = "AABBCCDDEEFFGGHH" fullword wide
70     $s14 = "inflate 1.2.8 Copyright 1995-2013 Mark Adler " fullword ascii
71     $s15 = " Type Descriptor" fullword ascii
72     $s16 = " constructor or from DllMain." fullword ascii
73     $s17 = " Base Class Descriptor at (" fullword ascii
74     $ex = "ping 127.0.0.1" ascii fullword
75   condition:
76     ( uint16(0) == 0x5A4D ) and
77     ( filesize > 70KB and filesize < 3MB ) and
78     ( 12 of them ) and
79     ( not $ex )
80 }

```




## Indicators of Compromise

---

00E415E72A4FC4C8634D4D3815683CE8 KingOfHearts (urlencode variant)  
4E2C2E82F076AD0B5D1F257706A5D579 KingOfHearts (JSON variant)  
AB956623B3A6C2AC5B192E07B79CBB5B QueenOfHearts  
4BBD5869AA39F144FADDAD85B5EECA12 QueenOfHearts  
4076DDAF9555031B336B09EBAB402B95 QueenOfHearts  
096F7084D274166462D445A7686D1E5C QueenOfHearts  
29AA501447E6E20762893A24BFCE05E9 QueenOfClubs  
97c6cfa181c849eb87759518e200872f JackOfHearts  
7DB4F1547D0E897EF6E6F01ECC484314 Screenshot capture utility  
60D78B3E0D7FFE14A50485A19439209B Malicious LNK  
90EF53D025E04335F1A71CB9AA6D6592 Keylogger

- [Backdoor](#)
- [Keyloggers](#)
- [Malware Descriptions](#)
- [Malware Technologies](#)
- [Steganography](#)
- [Targeted attacks](#)

#### Authors

-  [Ivan Kwiatkowski](#)
-  [Pierre Delcher](#)
-  [Félix Aime](#)

IAmTheKing and the SlothfulMedia malware family

---

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