ReconHellcat Uses NIST Theme as Lure To Deliver New BlackSoul Malware

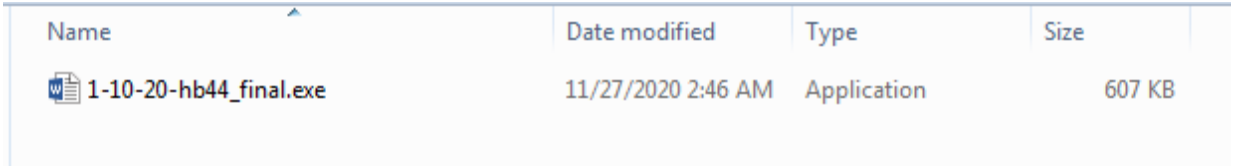
quointelligence.eu/2021/01/reconhellcat-uses-nist-theme-as-lure-to-deliver-new-blacksoul-malware/

January 6, 2021

Introduction

On 27 November, QuoIntelligence detected a new malware, seemingly uploaded to VirusTotal by a user in Turkmenistan, which shares multiple similarities to the threat actor we previously dubbed ReconHellcat. The campaign ultimately delivers a **previously undocumented remote access Trojan (RAT), which we dubbed *BlackSoul*.** After promptly alerting our customers, we notified Cloudflare about the C2 infrastructure hosted on their Workers service as per our responsible disclosure process.

Further analysis revealed the malware being part of a targeted campaign, that likely originated with a spear phishing email delivering a CAB archive. Both the CAB and the file contained within are named 1-10-20-hb44_final to impersonate one of the documents available on the National Institute of Standards and Technology (NIST) website.



Name	Date modified	Type	Size
1-10-20-hb44_final.exe	11/27/2020 2:46 AM	Application	607 KB

Figure 1: CAB archive contents

Specifications, Tolerances, and Other Technical Requirements for Weighing and Measuring Devices
https://www.nist.gov/system/files/documents/2019/11/05/1-10-20-hb44_final.docx
1.10. General Code Handbook 44 – 2020 Handbook 44 – 2020 1.10. General Code Table of Contents Page Section 1.10. General Code 1-3 G-A. Application 1-3 G-A.1. Commercial and Law-Enforcement Equipment. 1-3 G-A.2. Code Application. 1-3 G-A.3. Special and Unclassified E...

Figure 2: Legitimate NIST document URL and filename

Technical Analysis

Loader.ReconHellcat

File Name	1-10-20-hb44_final.exe
SHA256	3be1dd49f01e8b7ddf9af765693690d44356399b9e6043e51d5e13c82194b2a4
First Submission to VT	2020-11-27 10:41:21
First AV detection rate	Low (10/71)

During our analysis, we determined 1-10-20-hb44_final.exe is a malicious loader, which uses obfuscation similar to the variant observed in the previously reported ReconHellcat campaign delivering BlackWater malware. Another similarity is that the loader utilizes C2 infrastructure hosted on the Cloudflare Workers service. Following a successful C2 connection, the loader retrieves two files: (1) an executable named *blacksoul*, and (2) a Dynamic-Link Library (DLL) named *blacksoulLib*. Additionally, the loader opens Microsoft Word with the aforementioned legitimate document from the NIST website. Essentially, ReconHellcat uses this legitimate document as a decoy. The blacksoul and blacksoulLib files have compilation timestamps from 27 and 26 November, respectively.

BlackSoul

File Name	Bl4ck_S0ul6s5_1d7704b469.blacksoul
SHA256	c49cad471a61adb5ea8a6d260887d1dd7f22de75d1143ce2a72828842ef4bb52
First Submission to VT	2020-11-29 18:23:26
First AV detection rate	Low (18/71)

The second stage executable is a newly observed malware family, which we linked to the ReconHellcat threat actor. We named the malware “BlackSoul” to match its internal name, main class name, and file name.

```
; boost::detail::thread_data<class boost::_bi::bind_t<void, class boost::_mfi::mf0<void, class BlackSoul>, class boost::_bi::list1<class boost::_bi::value<cl
??_R1A@?0A@EA@?$thread_data@V?$bind_t@XV?$mf0@XVBlackSoul@@@_mfi@boost@@V?$list1@V?$value@PAVBlackSoul@@@_bi@boost@@@_bi@3@@_bi@boost@@@detail@boost@@8 dd of
                                        ; DATA XREF: .rdata:boost::detail::thread_data<boost::_bi::bind_t<void,boost::_mfi::mf0<void,BlackSoul>,boost::_bi::l
                                        ; reference to type description
                dd 1                    ; # of sub elements within base class array
                dd 0                    ; member displacement
                dd -1                   ; vftable displacement
                dd 0                    ; displacement within vftable
                dd 40h                  ; base class attributes
                dd offset ??_R3?$thread_data@V?$bind_t@XV?$mf0@XV[redacted]@@@_mfi@boost@@V?$list1@V?$value@PAVBlackSoul@@@_bi@boost@@@_bi@3@@_bi@boost@@@deta
```

Figure 3: Class name “BlackSoul”

The malware is a classical minimal RAT, which is capable of file transfers and running arbitrary commands. Through static analysis, we determined that the executable’s main loop supports handling the following commands from its C2 server:

	Command Field Names	Actions Taken
1	**params**	**Executes a command and return the result.**
2	url and path or media and alternativeText	Downloads file(s) from a URL and stores them in a destination on the machine. Creates a destination folder if it does not already exist.
3	paths	Likely retrieves a specified file from the machine and uploads it to the C2.
4	config	Updates the configuration file (UsrClass.json) which contains C2 server info and miscellaneous fields.

Table 1: BlackSoul Commands and Actions Taken

BlackSoul makes use of two files:

- **UsrClass.json:** Contains a JSON configuration. It is unclear if this file is mandatory or merely used to save existing configurations between invocations of BlackSoul.
- **UsrClass.data:** Observed as a DLL with an Init() export, which we refer to as blacksoulLib and will describe in depth in the next section.

BlackSoul uses information gathered by blacksoulLib to call back to the C2 over the RESTful Strapi protocol and JSON based data encoding.

The RAT’s string obfuscation applies only to strings in the main program but excludes strings of third-party compiled in libraries. BlackSoul additionally uses various other techniques for obfuscation. In particular, strings are constructed dynamically on the stack and deobfuscated with a variety of mechanisms, such as a fixed key XOR cipher and a Caesar cipher using variable shift values.

blacksoulLib

File Name	Bl4ck_S0ul6s5_faac59ebe2.blacksoulLib
SHA256	fdd310ce1b4f03a79f7a6eda8df793f4c0718766228a9a0700cf0b5a4ea648e2
First Submission to VT	2020-11-26 23:45:57
First AV detection rate	Low (18/71)

```
.rdata:10059AE8 ;
.rdata:10059AE8 ; Export Address Table for BlackSoulLib.dll
.rdata:10059AE8 ;
.rdata:10059AE8 off_10059AE8    dd rva Init             ; DATA XREF: .rdata:10059ADC↑o
.rdata:10059AEC ;
.rdata:10059AEC ; Export Names Table for BlackSoulLib.dll
.rdata:10059AEC ;
.rdata:10059AEC off_10059AEC    dd rva aInit            ; DATA XREF: .rdata:10059AE0↑o
.rdata:10059AEC                                         ; "Init"
.rdata:10059AF0 ;
.rdata:10059AF0 ; Export Ordinals Table for BlackSoulLib.dll
.rdata:10059AF0 ;
.rdata:10059AF0 word_10059AF0   dw 0                    ; DATA XREF: .rdata:10059AE4↑o
.rdata:10059AF2 aBlacksoullibDl db 'BlackSoulLib.dll',0 ; DATA XREF: .rdata:10059ACC↑o
.rdata:10059B03 aInit           db 'Init',0             ; DATA XREF: .rdata:off_10059AEC↑o
```

Figure 4: exports of the originally named blacksoulLib

The file is a DLL with a single export, Init(), which is called by BlackSoul. In this instance, its primary functions are:

- Searching the victim's machine for Firefox, Chrome, and Opera data. If the browser data is not found, the program terminates early.
- Decoding a C2 URL later used by BlackSoul
- Decoding a Cloudflare DNS-over-HTTPS (DoH) URL.
- Generating further login information for the C2 and returning gathered data to BlackSoul in JSON format, including:
    - A username with three random appended characters.
    - A password consisting of 24 random characters.

```
mov     [ebp+var_66], 33h ; '3'
mov     [ebp+var_65], 69h ; 'i'
mov     [ebp+var_64], 6Ah ; 'j'
mov     [ebp+var_63], 7Bh ; '{'
mov     [ebp+var_62], 34h ; '4'
mov     [ebp+var_61], bl
mov     al, [ebp+var_8D] ; https://shrill-wave-90be.0black.workers.dev/
mov     eax, ebx

loc_100055B8:
sub     [ebp+eax+var_8D], 5
inc     eax
cmp     eax, 2Ch ; ','
jb      short loc_100055B8

sub     esp, 10h
lea     eax, [ebp+var_8D]
mov     [ebp+var_F0], eax
mov     ecx, esp
lea     eax, [ebp+var_F0]
mov     [ebp+var_24], esp
push    eax
call    sub_10006FAC
mov     byte ptr [ebp+var_4], 4
mov     [ebp+var_14], 7Dh ; '}' ; url
mov     [ebp+var_13], 7Ah ; 'z'
mov     [ebp+var_12], 74h ; 't'
mov     [ebp+var_11], bl
mov     al, [ebp+var_14]
mov     eax, ebx

loc_100055FE:
sub     [ebp+eax+var_14], 8
inc     eax
cmp     eax, 3
jb      short loc_100055FE

lea     eax, [ebp+var_14]
push    eax             ; Src
lea     ecx, [ebp+var_EC]
call    create_value
mov     ecx, eax
mov     byte ptr [ebp+var_4], 3
call    set_value
```

Figure 5: C2 URL decryption and setting of the URL parameter

Based on our observations, the DLL's specific functionality adapts to various victims' environments, and the DLL outputs different C2 information for various targets.

Victimology

QuoIntelligence was unfortunately unable to uncover the entities targeted by this campaign. The only information at hand relies on:

- The VirusTotal submitter's country (Turkmenistan)
- The theme used as a lure (NIST)

Due to the limited information available to determine victimology, we cannot definitively state a target. However, it is likely that the BlackSoul campaign targeted a government-related body based on the theme lure, since NIST develops and publicizes security compliance standard for the US Federal Government and any organization who handles government data. As well, previously observed ReconHellcat campaign targets consisted of primarily defense and diplomatic government bodies.

Attribution

When we initially discovered ReconHellcat, its campaign characteristics and Tactics, Techniques, and Procedures (TTPs) were unique enough to classify it as a new threat actor. During our analysis of the new BlackSoul campaign, we identified limited yet sufficient similarities overlapping with the earlier observed BlackWater campaign. As a result, we have high confidence attributing this attack to ReconHellcat.

Similarities to earlier ReconHellcat campaigns:

- Lure themes of government related organization materials.
- Usage of compressed archives, likely via spear phishing email links or attachments, to distribute the initial attack artifacts.
- A three-stage attack scheme.

Similarities between ReconHellcat's BlackSoul and BlackWater malware:

- Supports DNS-over-HTTPS (DoH) using cloudflare-dns.com.
- Has clear internal naming likely due to a lack of artifact cleanup in the malware build process.
- Resolves the C2 hostnames via DNS over HTTPS (DoH) using a built-in feature of libcurl, aclient-side URL transfer library.
- Contains paths and parameters to use Strapi – a content management system (CMS).
- Identical string obfuscation.
- Uses Cloudflare Workers Service (*.workers[.]dev) to host C2 infrastructure.
- JSON–encoded communications.
- Similar kind of randomized login (user registration) scheme with the C2 server.
- Malware samples contain a 'Black' prefix in their naming schemes.

To note, although we have not found a strong correlation or technical link between ReconHellcat and APT28, there are shared characteristics between the two groups, which we highlighted in our recent APT28 reporting.

Appendix I – IOCs

hxxps://noisy-haze-af47.fromhell.workers.dev/uploads/Bl4ck_S0ul6s5_1d7704b469.blacksoul

hxxps://noisy-haze-af47.fromhell.workers.dev/uploads/Bl4ck_S0ul6s5_faac59ebe2.blacksoulLib

hxxps://shrill-wave-90be.0black.workers.dev/

Loader.ReconHellcat

3be1dd49f01e8b7ddf9af765693690d44356399b9e6043e51d5e13c82194b2a4

BlackSoul

c49cad471a61adb5ea8a6d260887d1dd7f22de75d1143ce2a72828842ef4bb52

blacksoulLib

fdd310ce1b4f03a79f7a6eda8df793f4c0718766228a9a0700cf0b5a4ea648e2

MITRE ATT&CK

TACTIC	TECHNIQUE
Initial Access	T1566: Phishing
Execution	T1204: User Execution
Defense Evasion	T1027: Obfuscated Files or Information
Credential Access	T1555: Credentials from Password Stores
Discovery	T1082 System Information Discovery
Collection	T1005: Data from Local System
Command and Control	T1132: Data Encoding T1105: Ingress Tool Transfer T1572: Protocol Tunneling

TACTIC	TECHNIQUE
Exfiltration	T1041: Exfiltration Over C2 Channel
	T1020: Automated Exfiltration

Do you want to stay informed of cyber and geopolitical threats targeting *your* organization? Are you interested in receiving exclusive and unpublished intelligence?

Get in touch!

Join Our Newsletter!

Subscribe to our newsletter to receive Weekly Intelligence Summaries, cyber news, and exciting updates!

Only valid business emails will be approved.

Join Our Newsletter!

Subscribe to our newsletter to receive Weekly Intelligence Summaries, cyber news, and exciting updates!

Only valid business emails will be approved.