# APT15 is Alive and Strong: An Analysis of RoyalCli and RoyalDNS

10 March 2018 By Matt Lewis

Research Reverse Engineering Threat Intelligence

In May 2017, NCC Group's Incident Response team reacted to an ongoing incident where our client, which provides a range of services to UK Government, suffered a network compromise involving the advanced persistent threat group APT15.

**APT15 is also known as, Ke3chang, Mirage, Vixen Panda GREF and Playful Dragon.**

A number of sensitive documents were stolen by the attackers during the incident and we believe APT15 was targeting information related to UK government departments and military technology.

## APT15 expands its arsenal

During our analysis of the compromise, we identified new backdoors that now appear to be part of APT15's toolset. The backdoor BS2005 – which has traditionally been used by the group – now appears alongside the additional backdoors RoyalCli and RoyalDNS.

The RoyalCli backdoor appears to be an evolution of BS2005 and uses familiar encryption and encoding routines. The name RoyalCli was chosen by us due to a debugging path left in the binary:

```
c:\users\wizard\documents\visual studio 2010\Projects\RoyalCli\Release\RoyalCli.pdb
```

RoyalCli and BS2005 both communicate with the attacker's command and control (C2) through Internet Explorer (IE) by using the COM interface IWebBrowser2. Due to the nature of the technique, this results in C2 data being cached to disk by the IE process; we'll get to this later.

Analysis ( r of
similar p l on
either Lir

All of the ipts in
order to e
Windows evade
behaviou ility.

Additiona eration
tool, the ita
dumping

spwebme oject
names fc ssue a
query to oup also
used key osoft
Exchange

APT15 wa lden
tickets. T on
actions b

## APT1

Upon eje r via the
corporat
compromised host.

This time, APT15 opted for a DNS based backdoor: RoyalDNS. The persistence mechanism used by RoyalDNS was achieved through a service called 'Nwsapagent'.

C2 of this backdoor was performed using the TXT record of the DNS protocol. C2 was communicating with the domain 'andspurs[.]com'.

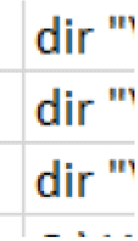
We mentioned earlier that due to the nature of the IE injection technique used by the HTTP-based backdoors, a number of C2 commands were cached to disk. We were able to recover these files and reverse engineer the encoding routine used by the backdoors in order to uncover the exact commands executed by the attacker.

In total, we were able to recover more than 200 commands executed by the attacker against the compromised hosts and were able to gain a clear insight into the attacker’s TTPs. Our decode scripts ca

Analysis ff the
land’. The nce
activities and
bcp.exe.

Lateral m the C$
share of ed a tool
known as scripts
and bina

During o ake,
shown be cuting
comman .



```
dir "
dir "
dir "
```

## IOCs

Below ar

```
Royal I
BS2005: 750d9eecd533f89b8aa13aeab173a1cf813b021b6824bc30e60f5db6fa7b950b
BS2005: 6ea9cc475d41ca07fa206eb84b10cf2bbd2392366890de5ae67241afa2f4269f
RoyalCli: 6df9b712ff56009810c4000a0ad47e41b7a6183b69416251e060b5c80cd05785
MS Exchange Tool: 16b868d1bef6be39f69b4e976595e7bd46b6c0595cf6bc482229dbb9e64f1bce
```

NCC Group Fox-IT have created a number of Suricata IDS rules to detect APT15 activity through the use of these backdoors. These, along with YARA signatures for the backdoors identified, can be found in the Github repository linked above.

# Domains

The RoyalCli backdoor was attempting to communicate to the following domains:

- News.me
- video.me

The BS20

- Run.linoc
- Singa.linc
- log.autoc

RoyalDN

- andspurs

Possible

- Micakiz.w
- cavanic9[
- ridingduc
- zipcodet
- dnsapp[.]

Written b

First pub

## This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

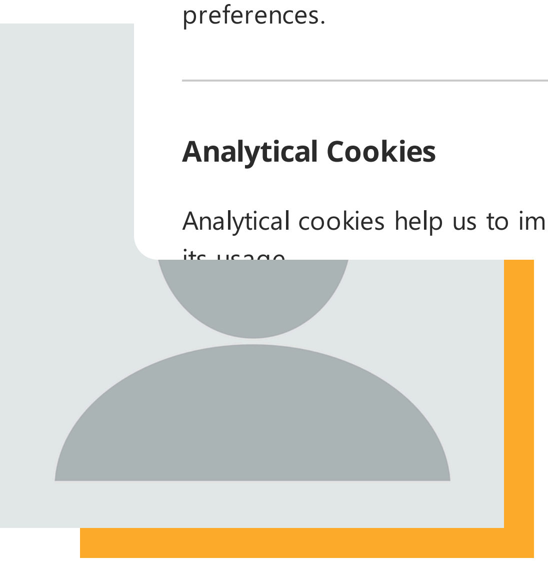
### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

### Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage



Terms an

Privacy P

Contact U

Hotline

© NCC Gr

## This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

### Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage