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 Governn group APT15.

APT15 is also known as

A number of sensitive o 5 was targeting information related to U

APT15 expa

During our analysis of t 15's toolset. The backdoor BS2005 – whic nal backdoors RoyalCli and RoyalDNS.

The RoyalCli backdoor a routines. The name RoyalCli was chosen by

```
c:\users\wizard\docume
```

RoyalCli and BS2005 bo Explorer (IE) by using the COM interface IWeb ed to disk by the IE process; we'll get to this

Analysis of the domains ssible domains, shown at the bottom of the po rence for using the ASN AS63949.

All of the backdoors identified – excluding RoyalDNS – required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved through the use of a simple Windows run key. We believe that APT15 could have employed this technique in order to evade behavioural detection, rather than due to a lack of sophistication or development capability.

Additional tools were recovered during the incident, including a network scanning/enumeration tool, the archiving tool WinRAR and a bespoke Microsoft SharePoint enumeration and data dumping tool, known as 'spwebmember'.

spwebmember was written in Microsoft .NET and includes hardcoded values for client project names for data extraction. The tool would connect to the SQL SharePoint database and issue a query to dump all data from the database to a temporary file affixed with 'spdata'. The group also used keyloggers and their own .NET tool to enumerate folders and dump data from Microsoft Exchange mailboxes.

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of remediation actions being undertaken, such as a password reset.

APT15 lives off the land

Upon ejection from the network, APT15 managed to regain access a couple of weeks later via the corporate VPN solution with a stolen VPN certificate, which they had extracted from a 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 can be found on our Github page: https://github.com/nccgroup/Royal_APT

Analysis of the commands executed by APT15 reaffirmed the group's preference to 'live off the land'. They utilised Windows commands in order to enumerate and conduct reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, net.exe, systeminfo.exe, ipconfig.exe and bcp.exe.

Lateral movement was conducted through by a combination of net command, mounting the C$ share of hosts and manually copying files to or from compromised hosts. APT15 then used a tool known as RemoteExec (similar to Microsoft's Psexec) in order to remotely execute batch scripts and binaries.

During our analysis of t ow in the folder name 'systme'. This indicates rface, rather than an automated or GUI proc

IOCs

Below are a number of

```
Royal DNS: bc937f6e958
BS2005: 750d9eecd533f8
BS2005: 6ea9cc475d41ca
RoyalCli: 6df9b712ff56
MS Exchange Tool: 16b8
```

NCC Group Fox-IT have of these backdoors. These, along with YARA inked above.

Domains

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

- News.memozilla[.]org
- video.memozilla[.]org

The BS2005 backdoor utilised the following domains for C2:

- Run.linodepower[.]com
- Singa.linodepower[.]com
- log.autocount[.]org

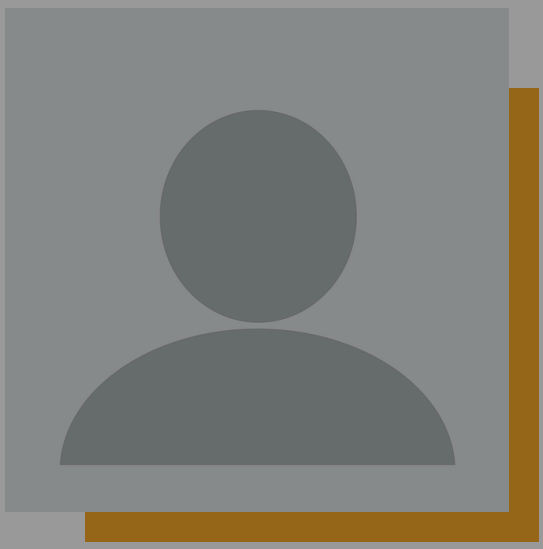
RoyalDNS backdoor was seen communicating to the domain:

- andspurs[.]com

Possible linked APT15 domains include:

- Micakiz.wikaba[.]org
- cavanic9[.]net
- ridingduck[.]com
- zipcodeterm[.]com
- dnsapp[.]info

Written by Rob Smallridge
First published on 10/03/18



Matt Lewis