APT15 is alive and strong: An analysis of RoyalCli and RoyalDNS

nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

September 3, 2018

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 of the domains and IP address infrastructure used by APT15 identified a number of similar possible domains, shown at the bottom of the post. These appeared to be hosted on either Linode or Google Cloud, with a preference 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'.

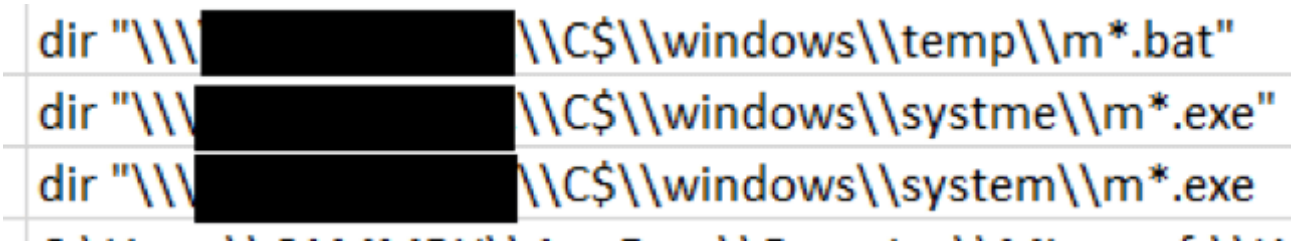
We mentioned earlier that due to the nature of the IE injection technique used by the HTTP-based backdoors, a number of C2 commands were cached to disk. We were able to recover these files and reverse engineer the encoding routine used by the backdoors in order to uncover the exact commands executed 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 the decoded attacker commands we noticed a typographical mistake, shown below in the folder name 'systme'. This indicates that a human operative was executing commands on a command line style interface, rather than an automated or GUI process.



IOCs

Below are a number of hashes relating to the backdoors identified in use by APT15

```
Royal DNS: bc937f6e958b339f6925023bc2af375d669084e9551fd3753e501ef26e36b39d>
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.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

Published date: 10 March 2018

Written by: Rob Smallridge