New tools uncovered from hacking group APT15

RoyalCLI and RoyalDNS backdoors discovered by NCC Group

NCC Group has discovered two previously unknown backdoors used by the elusive hacker group APT15, providing unique insight into its methods. The group is also known as K3chang, Mirage, Vixen Panda, GREF and Playful Dragon.

The global cyber security and risk mitigation expert was able to track the movements of the group over more than a year by decoding more than 200 commands from several compromised hosts, in turn understanding how APT15 uses bespoke tools to target victims.

In this instance, the attackers targeted a global company that provides multiple services to UK government. The attackers operated within the victim's network from May 2016 until late 2017, compromising over 30 hosts during that period. APT15 were targeting information related to UK government departments and sensitive communication technology.

By using the open-source tool Mimikatz, the attackers were able to gain domain administrator credentials aiding them in later stealing a VPN certificate which they used to access the victim's network remotely.

APT15 was then able to deploy three backdoors – BS2005, which has previously been documented by cyber security company FireEye, as well as RoyalCLI and RoyalDNS, which have not been discussed publically before. By looking at the reuse of this code, NCC Group researchers were able to link these backdoors to the same threat actor.

The RoyalCLI backdoor is similar to BS2005 in that it uses Windows command prompt (cmd.exe) to execute most of its commands. However, by copying the default cmd.exe and patching it, RoyalCLI is able to bypass policy settings that disable running of command prompt on the host machine.

In contrast, the RoyalDNS backdoor takes commands, runs them, then returns output using DNS. It differs from the other two backdoors found on the victim's network in that it installs itself persistently and communicates over DNS rather than HTTP.

Once inside the victim's network, the group was able to extract and collect information in multiple ways. The group used a tool called Comma Separated Value Data Exchange (CSVDE), which can export data in bulk from Microsoft Windows Active Directory, as well as Bulk Copy

Program (BCP), which comes with Microsoft SQL, to export data from Microsoft SQL databases.

These methods were combined with bespoke tools to extract information from Microsoft Sharepoint and Microsoft Exchange. In the case of the Microsoft Sharepoint tool the binary included hard coded project names that were specific to the victim.

Ahmed Zaki, senior malware researcher at NCC Group, said: “Through our investigation we were able to identify and monitor the attack process from start to finish, offering us unique insight into the behaviour of this group. It’s clear to see that this is a highly sophisticated threat actor that has no problem writing tools which are specific to its victims”.

“Knowledge sharing in the security industry is vital in order to improve the security posture and capabilities of the sector and UK as a whole. Discussing these types of insights is therefore necessary to ensure that we’re always able to understand and adapt to an ever-increasing variety of threats.”

ENDS

Published date: 10 March 2018

Filter By Service

- [ ] Software Escrow & Verification
- [ ]

Cyber Security

- [ ] Risk Management & Governance
- [ ] Website Performance
- [ ] Software Testing
- [ ] Corporate
- [ ] Business Insights
- [ ] Careers

Filter By Date

2018 (/uk/about-us/newsroom-and-events/press-releases/?Year=2018)

- March (1) (/uk/about-us/newsroom-and-events/press-releases/?Year=2018&Month=3)
- February (1) (/uk/about-us/newsroom-and-events/press-releases/?Year=2018&Month=2)
- January (7) (/uk/about-us/newsroom-and-events/press-releases/?Year=2018&Month=1)

2017 (/uk/about-us/newsroom-and-events/press-releases/?Year=2017)

2016 (/uk/about-us/newsroom-and-events/press-releases/?Year=2016)

2015 (/uk/about-us/newsroom-and-events/press-releases/?Year=2015)

2014 (/uk/about-us/newsroom-and-events/press-releases/?Year=2014)

Call us on:
+44(0)161 826 5867 (tel:+441618265867)

Board & Senior Management (/uk/about-us/what-we-do/board-and-executive-committee/)
Careers (/uk/about-us/careers/)
Resources (/uk/about-us/resources/)
Office Locations (/uk/about-us/what-we-do/office-locations/)

Investor Relations

Share Price (/uk/about-us/investor-relations/share-price/)
Results & Presentations (/uk/about-us/investor-relations/results-and-presentations/)
Stock Exchange Announcements (/uk/about-us/investor-relations/stock-exchange-announcements/)

Legal

Terms & Conditions (/uk/about-us/terms-and-conditions/)
Privacy Policy (/uk/about-us/privacy-policy/)
Cookie Policy (/uk/about-us/privacy-policy/cookie-policy/)
Accessibility (/uk/about-us/accessibility/)
Sitemap (/uk/sitemap/)

Latest from @NCCGroupplc (https://twitter.com/NCCGroupplc)

COOK, a provider of high-quality frozen meals, suspected that slow load times were negatively affecting its business. Download our case study for an in-depth analysis on how NCC Group measured and improved the performance of COOK's website https://www.nccgroup.trust/uk/about-us/resources/cook-real-user-monitoring-case-study/?resources=Case+Studies … (https://t.co/Zu4HptA4Ut)
Reply (https://twitter.com/intent/tweet?in_reply_to=973944510173597696) Retweet (https://twitter.com/intent/retweet?tweet_id=973944510173597696) Favorite (https://twitter.com/intent/favorite?tweet_id=973944510173597696)

Despite the fact #GDPR (https://twitter.com/hashtag/GDPR?src=hash) will be enforced from May 2018, many organisations remain unclear on the topic of breach notification under #GDPR (https://twitter.com/hashtag/GDPR?src=hash). For best practice advice on how to communicate a personal data breach download our ebook now https://www.nccgroup.trust/uk/our-research/ebook-breach-notification-under-gdpr-how-to-communicate-a-personal-data-breach/?research=Whitepapers … (https://t.co/ENg7QQ7Ob4)
Reply (https://twitter.com/intent/tweet?in_reply_to=973891662408765441) Retweet (https://twitter.com/intent/retweet?tweet_id=973891662408765441) Favorite (https://twitter.com/intent/favorite?tweet_id=973891662408765441)