Who was behind this unprecedented Cyber attack on Western infrastructure?

intrusiontruth.wordpress.com/2018/07/17/who-was-behind-this-unprecedented-cyber-attack-on-western-infrastructure/

intrusiontruth July 17, 2018

In late 2016, Cyber threat analysts in PwC and BAE Systems began assisting victims of a new global cyber espionage campaign. They named the campaign Operation Cloud Hopper.

Cloud Hopper turned out to be an attack of unprecedented scale that targeted companies known as “managed IT service providers”, or MSPs. Because MSPs manage the IT systems of hundreds of clients, the technique used by the Cloud Hopper attackers was highly effective – they gained access not only to the sensitive data of the MSPs themselves, but also to their clients globally.

By attacking a handful of companies, the Cloud Hopper actors gained access to potentially thousands of networks.

Executive summary

Since late 2016, PwC UK and BAE Systems have been assisting victims of a new cyber espionage campaign conducted by a China-based threat actor. We assess this threat actor to almost certainly be the same as the threat actor widely known within the security community as 'APT10'. The campaign, which we refer to as Operation Cloud Hopper, has targeted managed IT service providers (MSPs), allowing APT10 unprecedented potential access to the intellectual property and sensitive data of those MSPs and their clients globally. A number of Japanese organizations have also been directly targeted in a separate, simultaneous campaign by the same actor.

We have identified a number of key findings that are detailed below.

APT10 has recently unleashed a sustained campaign against MSPs. The compromise of MSP networks has provided broad and unprecedented access to MSP customer networks.

- Multiple MSPs were almost certainly being targeted from 2016 onwards, and it is likely that APT10 had already begun to do so from as early as 2014.
- MSP infrastructure has been used as part of a complex web of exfiltration routes spanning multiple victim networks.

APT10 has significantly increased its scale and capability since early 2016, including the addition of new custom tools.

- APT10 ceased its use of the Poison Ivy malware family after a 2013 FireEye report, which comprehensively detailed the malware's functionality and features, and its use by several China-based threat actors, including APT10.
- APT10 primarily used PlugX malware from 2014 to 2016, progressively improving and deploying newer versions, while simultaneously standardising their command and control function.
- We have observed a shift towards the use of bespoke malware as well as open-source tools, which have been customised to improve their functionality. This is highly likely to be indicative of an increase in sophistication.

Infrastructure observed in APT10's most recent campaigns links to previous activities undertaken by the threat actor.

- The command and control infrastructure used for Operation Cloud Hopper is predominantly dynamic-DNS domains, which are highly interconnected and link to the threat actor's previous operations. The number of dynamic-DNS domains in use by the threat actor has significantly increased since 2016, representative of an increase in operational tempo.
- Some top level domains used in the direct targeting of Japanese entities share common IP address space with the network of dynamic-DNS domains that we associate with Operation Cloud Hopper.

APT10 focuses on espionage activity, targeting intellectual property and other sensitive data.

- APT10 is known to have exfiltrated a high volume of data from multiple victims, exploiting compromised MSP networks, and those of their customers, to stealthily move this data around the world.
- The targeted nature of the exfiltration we have observed, along with the volume of the data, is reminiscent of the previous era of APT campaigns pre-2013.

PwC UK and BAE Systems assess APT10 as highly likely to be a China-based threat actor.

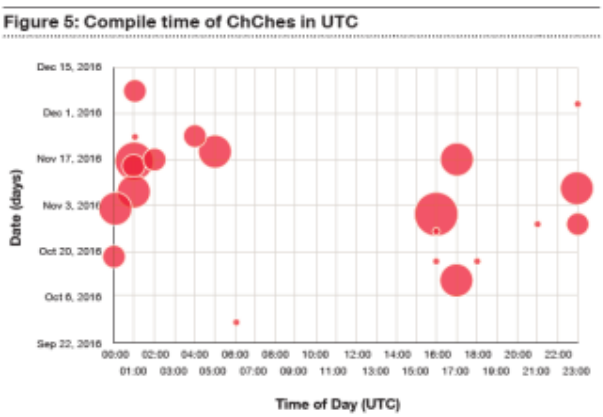
The Cloud Hopper analysis by PwC and BAE Systems

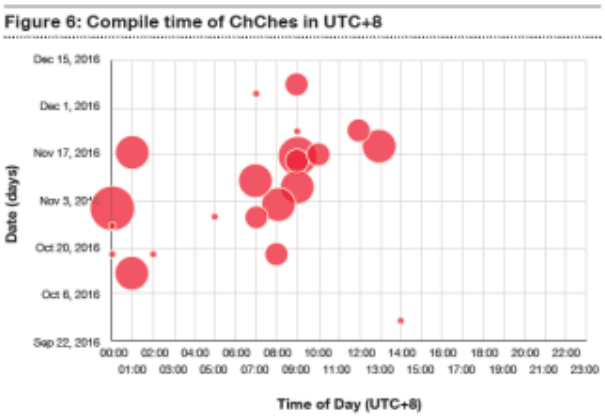
APT10 was behind Cloud Hopper

PwC and BAE assessed that Operation Cloud Hopper was almost certainly managed by the threat actor known within the Information Security community as “APT10”. This assessment was based on the group’s highly interconnected network of infrastructure, which had connections with APT10’s previous operations. The Palo Alto Networks report menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations shows that a series of old APT10 command and control (C2) domains (including cmdnetview[.]com) associated with servers that were later used by the Cloud Hopper group.

The Cloud Hopper report released by PwC and BAE assessed that APT10 had significantly increased its scale and capability since early 2016 and was focused on espionage activity by targeting intellectual property and other sensitive data.

It was also assessed at the time that APT10 was highly likely to be a China-based threat actor, based on a series of clues including the compile times of binaries, registration times of domains, activity indicating a pattern of work in line with China Standard Time and a mix of diplomatic and political targets being closely aligned with China’s strategic interests.





Cloud Hopper analysis showing activity during working day in UTC+8 timezone

So what?

Analysts working with this blog have spent the last year investigating the most damaging attacks to hit Western companies, starting with APT10.

We have identified a number of individuals behind the attack and the companies with which they have been associated.

We plan to tell the story – check back for more over the next month…