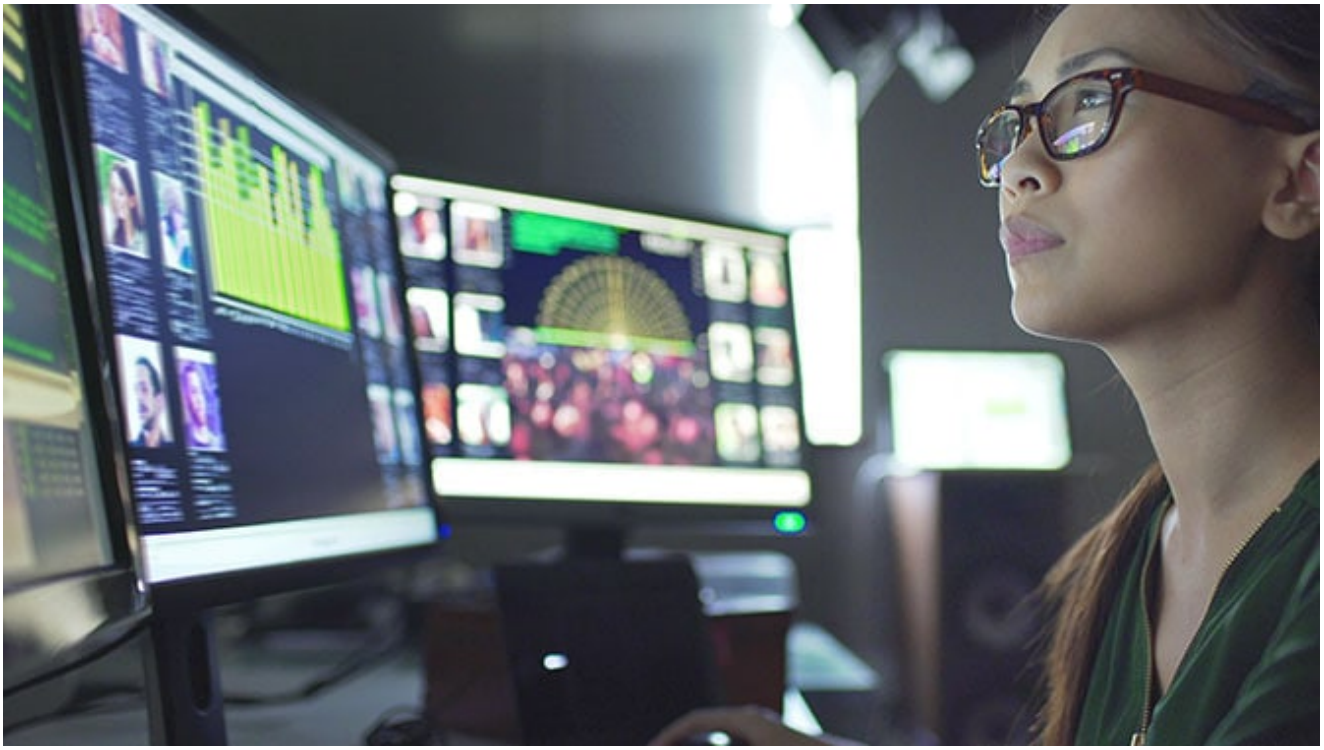
Tracking ‘Kimsuky’, the North Korea-based cyber espionage group: Part 2

pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html



Copy link

09 March, 2020

In 2019, PwC observed an increase in activity by North Korea-based threat actor Black Banshee, also known as ‘Kimsuky’.

In our previous blog, we examined some of the tradecraft exhibited by Black Banshee in its infrastructure setup. We discussed the threat actor’s reliance on certain IP ranges and domains, as well as its naming conventions for malicious domains and command and control server paths.

In this article we look at how the threat actor’s 2019 campaigns (even those continuing into 2020) can be broadly grouped into three main “clusters” – and how all these, in turn, are complementary to its overarching strategic objectives in the context of current international relations.

Clustering activity

Investigating Black Banshee's 2019 activity, and the infrastructure patterns emerging across different campaigns and connecting them, we identified a number of activity "clusters". Such clusters of campaigns and operations – identified based on our own datasets as well as excellent open source research from others – are tied together by infrastructure links, similar tradecraft, shared indicators, and matching targeting.

Figure 1 below shows the activity of several campaigns – grouped into such clusters – between November 2018 and February 2020:

- The WildCommand cluster;
- The BabyShark cluster; and,
- A credential harvesting cluster.

Figure 1. A high-level overview of campaigns conducted by Black Banshee throughout 2019.
The dotted lines in the picture mark periods in which PwC analysts did not observe large volumes of activity related to a certain campaign, but in which such activity was likely in preparation, or still ongoing.

The Wild Cluster

The WildCommand cluster includes the activity first publicly detailed in AhnLab's Operation Kabar Cobra. The continuation of that activity was exposed in ThreatRecon's Operation Kitty Phishing. We tracked this campaign as it continued throughout April and May 2019.

All this activity targeted the South Korean government sector, as well as aerospace and defence contractors and cryptocurrency organisations doing business in South Korea. Based on our analysis, we assessed that the operations were effectively part of the same overarching campaign, as they exhibited extensive overlaps in infrastructure and correspondence in tools, techniques and procedures (TTPs) deployed – including a new malware family at the time, a Remote Access Trojan (RAT) that we referred to as WildCommand.

Figure 2. An evolution: Operation Kabar Cobra, Kitty Phishing, WildCommand and Missiles and Money are snapshots in time of a longer effort by Black Banshee.

We found further infrastructure links tying the WildCommand cluster to a campaign targeting cryptocurrency organisations, and active from 2018 until at least May 2019, which EST Security has grouped under the name "Operation MoneyHolic".

We also saw multiple infrastructure connections between the WildCommand cluster and yet another set of activity, dated around May 2019, leveraging a DLL RAT family that we refer to as MyDogs. MyDogs – a RAT that uses FTP to receive commands and exfiltrate files – was reported on as being used in a cluster of activity called "Operation Red Salt" by AhnLab, in a campaign mostly targeted towards South Korean entities. Although the set of activity that AhnLab called Operation Red Salt was active around July 2019, we observed the leadup for this campaign building from at least May 2019 – around the time when we also noticed a temporary halt in the activity associated with Operation WildCommand.

Recently, we have observed new WildCommand activity. This return of the WildCommand campaign used similar TTPs to previous activity and a slightly updated version of the backdoor, with samples compiled around 13th February 2020; from what we have been able to observe so far, this activity targeted financial sector entities in South East Asia.

The BabyShark cluster

The second cluster that PwC identified across Black Banshee's 2019 activity revolves around a campaign, active since at least late 2018, that Palo Alto's Unit42 called "BabyShark" and EST Security refers to as "Operation SmokeScreen". This campaign has consistently targeted policy and national security think tanks as well as government entities in the US, South Korea, and European countries. It has also targeted organisations in the cryptocurrency space.

We noted infrastructure overlaps and indicator sharing between this and Prevailion's "Autumn Aperture" report, including similar malware and the same author name – "windosmb" – present across multiple lure documents utilised in both campaigns. Such evidence led us to assess that the Autumn Aperture campaign likely constituted a continuation of the BabyShark campaign.

Figure 3. An example of overlaps between PwC reporting on BabyShark activity, Operation SmokeScreen, Prevailion's Autumn Aperture campaign report, and ANSSI's advisory on credential phishing activity attributed to Black Banshee.

Figure 4. The continuum of BabyShark activity between November 2018 and December 2019.

BabyShark activity often relied on compromised infrastructure instead of adversary-registered domains. However, the naming of server-side folders remained consistent across BabyShark campaigns. Folders like "/customize/1111", server-side files like "cow.php", "expres.php", and malware parameters like "op=" remained characteristic of BabyShark malware through its iterations until the current time.

PwC analysts have routinely observed such server-side scripts on Black Banshee C2 infrastructure. These same server-side scripts were also observed in the context of a campaign targeting the South Korean government and dubbed "Operation Stealth Power" by EST Security. Although Operation Stealth Power was not directly linked to BabyShark activity, the use of those same scripts effectively ties together different Black Banshee campaigns based on the same infrastructure management TTPs.

A net cast wide: long-running, large-scale credential capture campaign

Separately, Prevailion noted some shared indicators and infrastructure connecting the "Autumn Aperture" campaign with activity discussed in a report by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), and also covered by Anomali in a late August 2019 report. Multiple infrastructure connections (examples of which are shown in Figure 4 above) and targeting similarities between the BabyShark campaign, Autumn Aperture, and the ANSSI report, lead us to assess these sets of activity are likely part of the

same “cluster”. This is an overarching effort to target mainly foreign governments as well as institutions in the national security, policy, and education space – with multiple similarities across the domains that we observed being set up between August and December 2018.

Conclusion

Both the WildCommand and BabyShark activity cluster – as well as the credential harvesting campaigns that PwC, ANSSI and Anomali have been tracking since at least 2018 – mainly targeted entities and organisations in South Korean and the United States. These campaigns’ operations focused on the following targets:

- Government (especially foreign governments, ministries, and diplomatic missions);
- National security (especially with regards to national security policy, defence, and North Korea-related affairs);
- Aerospace and defence,
- International relations and sanctions;
- Nuclear-related policy; and,
- Academia and research (especially in the nuclear space).

In this two-part series, we demonstrated how – within the horizon of PwC’s intelligence and visibility, as well as of open source research – most of the campaigns conducted by Black Banshee in 2019 actually turned out to be interlinked, in terms of:

- Infrastructure overlaps crossing over multiple campaigns and betraying the threat actor’s overall modus operandi; and,
- Overall mission objectives, showing consistent targeting by Black Banshee.

We have seen Black Banshee introduce new tooling (like the WildCommand and MyDogs RATs, and BabyShark malware), and assess it is likely that the threat actor will continue updating its toolset in upcoming campaigns.

However, as we saw throughout 2019, Black Banshee continues to rely on a series of tried-and-tested mechanisms, with distinctive operational tradecraft that emerges across its campaigns. Going into 2020, we have not observed this activity decreasing or becoming less aggressive, nor do we expect it do so – in fact, we expect Black Banshee to continue ramping up operations, especially in the face of the current international state of heightened tension.

Contact us

Contact us

Form

Hide