Tracking ‘Kimsuky’, the North Korea-based cyber espionage group: Part 1

pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.html

Copy link

18 February, 2020

For years, we have tracked the espionage threat actor we call Black Banshee (also known in open source as Kimsuky). In 2019, it launched multiple parallel cyber espionage campaigns, from large-scale credential harvesting to narrowly targeted espionage and exfiltration operations.

The foundations for this activity began in August 2018, when we observed Black Banshee setting up a substantial number of domains impersonating organisations across the government, academia, and policy sectors. This formed the basis for multiple spear-phishing and credential harvesting campaigns.

In tracking Black Banshee, we have identified a number of highly characteristic elements of the threat actor’s tools, techniques, and procedures (TTPs). In the two parts of this retrospective look at Black Banshee’s 2019 activity, we will:

- Examine the overlaps in Black Banshee's infrastructure and modus operandi that have allowed us to connect multiple strands of its operations more clearly than detailed so far in open source;
- Connect its 2019 campaigns, linking to activity dating back to late 2018; and,
- Highlight how it has operated to achieve certain strategic objectives.

Tradecraft: most used domains and naming conventions

Infrastructure connections: IP addresses

Firstly, let us dive into Black Banshee's mannerisms in setting up its infrastructure. Across 2019, it was possible to tie together different Black Banshee campaigns through the IP addresses used. For example, on numerous occasions command and control domains for Black Banshee malware resolved to IP addresses in following ranges - 185.224.137[.]0/23 and 185.224.138[.]0/23

The address 185.224.137[.]164, for one, has been used since at least December 2018 and up to January 2020 to serve at least 24 malicious Black Banshee domains, including (but not limited to):

- user-daum-centre[.]pe[.]hu (from 2019-04-15 to 2019-05-21);
- rrnaver[.]com (from 2019-08-21 to 2020-01-01); and,
- nortice-centre[.]esy[.]es (from 2020-01-02 to 2020-01-28).

It also hosted, between June and November 2019, the domain kakao-check[.]esy[.]es, which served as command and control (C2) for a sample of a new malware family that we call MyDogs – a RAT thought to be unique to Black Banshee, and which was first reported on in open source by AhnLab as part of its analysis on Operation Red Salt.[1]

Figure 1. 185.224.137[.]164 is an example of an IP that has hosted numerous Black Banshee domains – associated with different campaigns – throughout 2019 and into 2020. Some of these domains are shown here.

Infrastructure connections: domains

Among the domains used by Black Banshee, a few stood out for frequency across its campaigns.

- pe[.]hu - numerous subdomains on this domain were used in Operation Kabar Cobra, Operation Kitty Phishing, and Operation WildCommand; additional subdomains were listed in a Financial Security Institute VirusBulletin report detailing the tradecraft of numerous operations attributed to Black Banshee;[2]

- hol[.]es - subdomains on this domain were used for both the WildCommand cluster and Operation MoneyHolic. Incidentally, some of the malware involved in Operation MoneyHolic were samples of MyDogs malware, which was also used in Operation Red Salt;
- esy[.]es - subdomains on esy[.]es further strengthen the connections in infrastructure setup between the WildCommand cluster and Operation MoneyHolic, as well as overlaps with the infrastructure used for MyDogs malware used in Operation Red Salt; and,
- 890m[.]com - subdomains on 890m[.]com were implicated in the WildCommand cluster, as well as in activity using KONNI that had ties to Black Banshee[3], and in other Black Banshee activity.

While these domains are available for anyone to use, and not all of their subdomains are malicious, Black Banshee used subdomains on these domains multiple times across different operations. Other North Korea-based threat actors, especially APT37/Reaper, have also made use of some of the same domains (such as hol[.]es[4], 890m[.]com[5]) throughout 2019.

Figure 2. A high-level overview of some of the connections between different 2019 Black Banshee campaigns.

Infrastructure connections: naming

Even where the subdomains' parent domain was not the same, our analysts noticed a pattern of naming in adversary-registered infrastructure. We saw Black Banshee go down three main routes for domain naming:

1. Naming highly specific to an organisation or institution being targeted or impersonated (and often used for credential phishing);
2. Keywords referring to software used specifically in South Korea, often combined with more generic, office- or enterprise-related themes; and,
3. Seemingly generic names, including ones impersonating email services, or domains with similar or incremental numbering.

Black Banshee was also consistent in the setting up of command and control server-side folders:

- "/Est/up" and "/Est/down" were server-side paths seen in Operation Kabar Cobra, Operation Kitty Phishing, and Operation WildCommand – folders to stage files uploaded or downloaded by infected machines. We observed a similar server-side path (http://nortice-centre[.]esy[.]es/down/) being referred to by a new sample of a Black Banshee Windows Script File downloader first seen on 31 December 2019; this likely indicates that the threat actor is maintaining a consistent approach to infrastructure management and naming.

- The server-side path "/bbs/data/temp" was observed in both Operation Kabar Cobra and Operation Kitty Phishing.
- Its parent path, "/bbs/data", was observed in the context of Operation Red Salt, with one of the sub-folders associated with malware that was later tied by ESTSecurity to KONNI. Additionally, the same path was also observed on APT37/Reaper command and control servers.[6]
- Finally, "/bbs/filter" was present on a C2 for MyDogs malware related to Operation Red Salt.

In Summary

In tracking North Korea-based threat actor Black Banshee (also known as Kimsuky), we observed the threat actor display a series of infrastructure set-up habits. These included the use of specific IP ranges to set up actor-controlled command and control domains, the naming conventions used for such domains, and server-side folder names consistently reused by Black Banshee across its C2s.

Such habits and TTPs effectively allowed us to connect multiple campaigns through direct links and similarities in command and control infrastructure.

But that's not all. Having connected multiple Black Banshee's operations across 2019, we observed that distinct "clusters" of activity appeared – groups of campaigns and operations tied together by infrastructure links, similar tradecraft, shared indicators, and matching targeting.

In an upcoming blog, we will detail the connections between campaigns found across these clusters and offer strategic insight about their coherence in terms of TTPs and objectives.

---

1. 'Security Issue: Analysis Report on Operation Red Salt', in 'ASEC Report Vol. 96 Q3 2019', AhnLab
2. 'Kimsuky: Tracking the King of the Spear-Phishing', Jaeki Kim, Kyoung-Ju Kwak, Min-Chang Jang, VirusBulletin (4th October 2019)
3. 'Commonalities found between APT Groups, Konni and "Kimsuky"', EST Security (10th June 2019)
4. CTO-TIB-[illegible] – Reaper's Hooks
5. CTO-TIB-2019042[illegible]-01A – NOKKI against Norway
6. 'Detailed Analysis of Red Eyes Hacking Group', AhnLab, May 2018

Related content

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

In 2019, PwC observed an increase in activity by North Korea-based threat actor Black Banshee. Investigating Black Banshee's 2019 activity, we identified a...

Contact us

Contact us

Form

Hide