The many personalities of Lazarus

risky.biz/laz/

OpEd: North Korea's "Lazarus Group" is best understood as a network of distinct groups or "clusters", each with unique capabilities and quirks.

By Daniel Gordon and Brett Winterford · October 28, 2020

When it comes to North Korean cyber activity, analysts fall into one of two camps: The “it’s all Lazarus” camp or the “it’s complicated camp”. We’re in the second camp: DPRK activity should be clustered among a few related groups.

The DPRK doesn’t make this clustering easy. It’s often hard to know where the state-directed activity stops and the operator side-hustles start. We know the North Korean crews target cryptocurrency wallets and exchanges, but the split of the bounty/booty between the operators’ personal crypto-stashes and government coffers is a bit of a mystery.

Further, all the North Korean groups we list in this article use wipers or ransomware, and all use similar packers to mask malicious files. But overlapping geography and TTPs doesn’t mean a single “Lazarus Group” is orchestrating all these attacks. The overlaps are better explained by several operators sharing malware developed by a single team.

Now, we could sit back and go all angry panda whenever we see an analyst get it wrong, or we could have our own crack at defining who’s who in the zoo. Bucketing the activity provides a clearer picture of North Korea’s targeting habits and the risks that they pose so we can better predict and defend against them.

But first, a few caveats: linking the names different analysts give to each cluster of activity doesn’t make those groups synonymous. It’s a loose equivalency, at best. And our attempts to assign these groups some personality, well, that just makes our lives more bearable.

“The Lazarus Group”

aka Temp.Hermit, Labyrinth Chollima, RGB-D3, ZINC, Covellite, NICKEL ACADEMY

Let's start with the group that always gets the headlines. The Sony Hackers. The Bangladesh Bank SWIFT heist. Attempts to hack U.S. defense contractors. And according to the DoJ's Park indictment, the group responsible (if only in part) for WannaCry 2.0.

Because of the clustering problems described earlier, it's difficult – based on what's published – to know where this crew stops and all the others begin. For example, some researchers group all activity directed at banks under BlueNoroff (see below), others fold it under Lazarus.

What historically made Lazarus distinct – less so as time passes, were techniques (such as protocol impersonation) used in its malware.

Image Source: CISA

Lazarus has strong associations with the Fallchill remote access tool for Windows and similar capabilities that target MacOS, Android, and Linux. More recently it has been linked with multi-platform malware frameworks and fileless malware campaigns.

Lazarus is connected to a long-running, global campaign in which attackers built rapport with targets by posing as recruiters on LinkedIn, as well as campaigns that targeted the U.S electric sector.

It has generated revenue through attacks on cryptocurrency exchanges, but has of late tried its luck with BEC invoice fraud (in the midst of a suspected espionage operation), Magecart-style transaction skimming and big game ransomware attacks that use VHD malware.

"APT38"

aka BlueNoroff, Stardust Chollima, BeagleBoyz, NICKEL GLADSTONE

Now let's talk about the Dear Leader's primary breadwinners. APT38 are probably the most successful bank robbers in history.

While reporting on BlueNoroff and APT38 typically describe activity that uses the same tools and infrastructure as Lazarus, APT38 uses custom tools (ELECTRICFISH, PowerRatankba, PowerSpritz and job application-themed lures) in jobs entirely focused on generating

revenue.

Banks are attacked via watering hole attacks and ATM jackpotting. There's a growing body of evidence that the group is able to scale its operations by purchasing access to systems previously infected by TrickBot, and by using commercially available tools like PowerShell Empire and Cobalt Strike once they have a foothold.

And it's all handled with the kind of planning and care you'd expect from a heist movie: they usually go to some effort to cover their tracks, even if that means covering them with ransomware or a destructive attack.

"Andariel"

aka Silent Chollima, Dark Seoul, Rifle, Wassonite

Andariel is a bully. What it lacks in sophistication, it makes up for in belligerence.

This crew engages in espionage, but also gets tasked with disrupting and wiping things. A 10-day assault on South Korea in 2011 set a troubling new precedent for what pain the pariah state was prepared to inflict on their adversaries.

Andariel knows how to get noticed in all the places it probably shouldn't. It is one of the few groups bold enough to take aim at military targets in the U.S. and South Korea or to go after AV management servers on a victim's network. "YOLO, lets hack a nuclear plant and leave admin credentials hardcoded in the malware." And while we don't know who the hell 'Hack Hound' is, Andariel has some nasty things to say about them.

But like all the DPRK groups, there's a little cybercrime on the side, such as stealing from online gambling sites or ATMs in South Korea or India. It probably doesn't end there.

"APT37"

aka Group123, Ricochet Chollima, RedEyes, Reaper, ScarCruft, Geumseong121

APT37 is the wannabe hipster of DPRK's hacking elite: they are constantly upskilling ("I just earned my 0-day badge!") while actively trying to emulate DarkHotel, a thoroughly more capable actor.

APT37 often goes after individuals, as opposed to organisations. It has a taste for North Korean defectors, journalists and human rights activists. While mostly relying on spear phishing using Office or Hangul (Korean language) Word Processor (HWP) maldocs, they've also used torrent sites to deliver malware and been tied to a couple of strategic web compromises.

APT37 uses malware described by different intel shops as "Redoor", "DOGCALL", "ROKRAT" or "Final1stspy", as well as Android malware named Kevdroid.

Even when they went after sports fans, the attack looked inspired by the major leaguers. Can't these kids do anything original?

"Kimsuky"

aka Velvet Chollima, THALLIUM, TEMP.Firework, RGB-D5, Black Banshee

Kimsuky is called the "King of Spearphishing". Like most fishermen, they leave a stench: their OPSEC is pretty amateur.

Kimsuky has been pinned for going after the South Korean government and Chinese organisations, an attack related to the Korea Hydro & Nuclear Plant, and phishing attacks against U.S. military interests.

Kimsuky is also known for its "cowboy" loaders: part of an infection chain linked to attacks on U.S. academia and U.S. think tanks that used the BabyShark and KimJongRAT implants. (Malware RE isn't that much fun, so naming malware provides some light relief).

Wiser analysts have broken Kimsuky up into more specific clusters, to separate out standalone credential phishing campaigns that don't make use of this malware, for example.

Another cluster, named CERIUM by Microsoft, targeted pharmaceutical firms working on COVID-19 vaccines.

There are claims of Kimsuky using Konni malware and vice versa, but it's best to stay away from the mess that is Konni if you possibly can.

"DarkHotel"

aka Shadow Crane, DUBNIUM, TUNGSTEN BRIDGE, APT-C-06

Just kidding! Despite a number of people messing this up, DarkHotel is NOT DPRK. We're listing it here as a lesson on the limits of malware analysis for attribution.

Don't make this mistake. We will find you.

So that's it. We hope you've found this summary helpful. We'll update it every now and then as new research comes to light. Hints, corrections and suggestions are welcome at editorial@risky.biz.