A Look into the Lazarus Group's Operations

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations

What do the 2014 Sony hack and the 2016 Bangladeshi bank attacks have in common? Aside from being two of the most noteworthy cybercrime incidents of the past few years, these seemingly unrelated attacks are tied together by a common thread: their perpetrator, a cybercrime group called Lazarus.

Few cybercrime groups throughout history have had as much disruptive power and lasting impact as the Lazarus Group. Ever since their first attacks, which involved DDoS operations against various organizations across different industries, the group has managed to step up their attacks even further. Two of the group's most notable campaigns include the 2014 Sony hack, which involved sensitive company and personal information, and the 2016 Bangladeshi bankattack that stole millions of dollars from the financial institution. Recently, the group was seen expanding into cryptocurrency attacks, with the use of the RATANKBA malware to target cryptocurrency companies

Timeline of Lazarus Group Activities

The Lazarus group has had multiple operations over the years, most of which involve either disruption, sabotage, financial theft or espionage. The organization also has “spin-off” groups, which focus on specific kinds of attacks and targets:

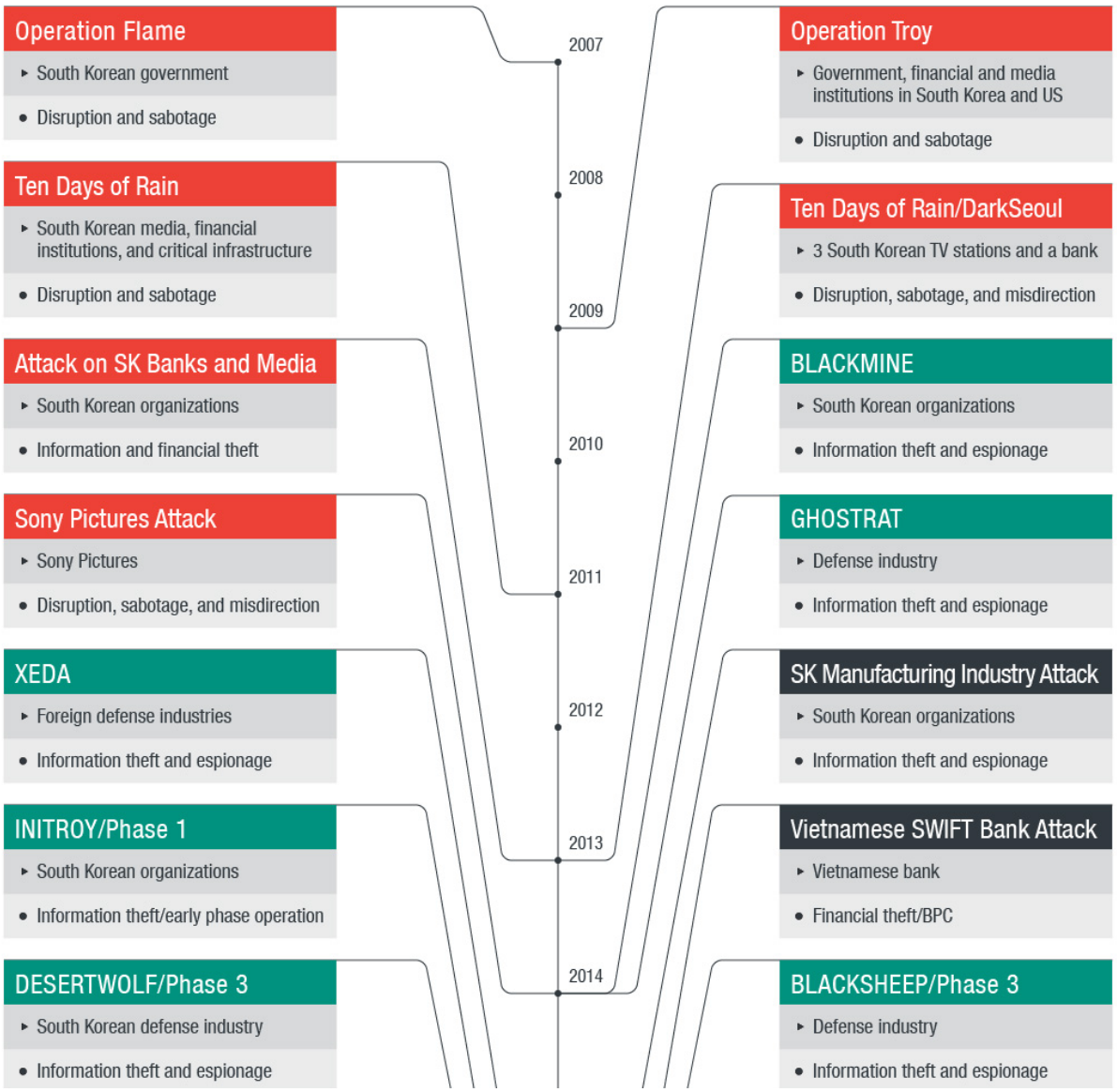
***Bluenoroff*:**

A subgroup focused on attacking foreign financial institutions. They are responsible for a wide array of financial theft incidents, including the aforementioned attack on a Bangladeshi bank.

***Andariel*:**

A subgroup focused on South Korean organizations and businesses using specifically tailored methods created for maximum effectivity.

The chart below shows a timeline of the group’s activities and objectives over the years.



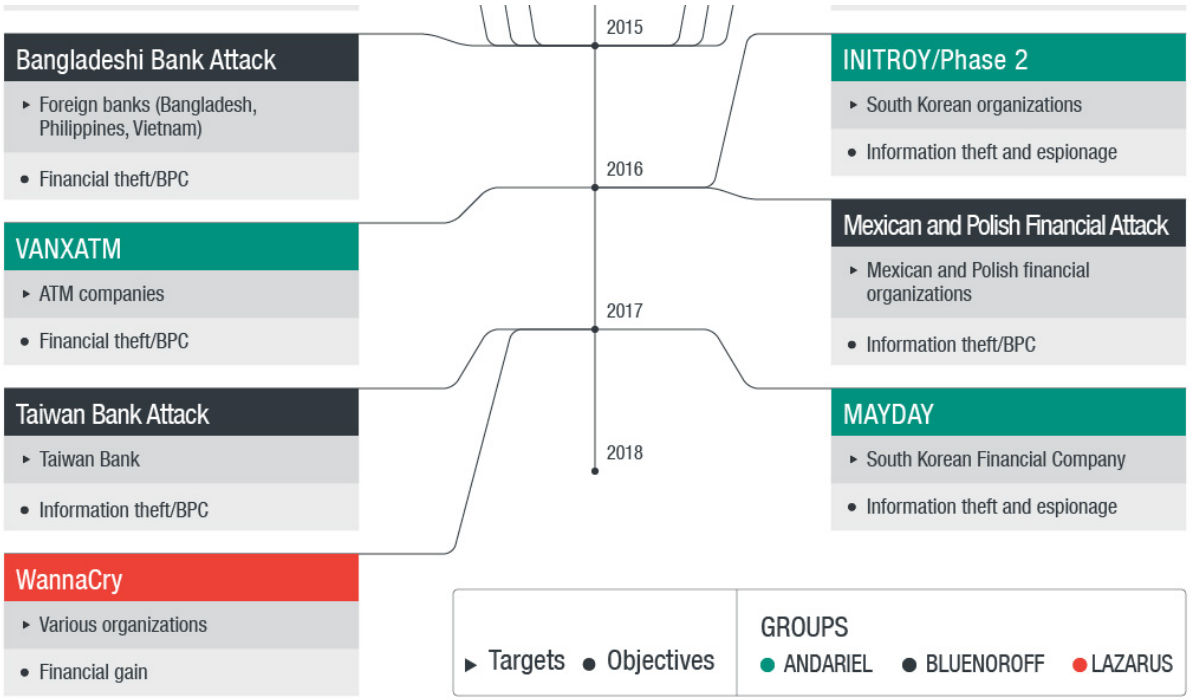


Figure 1: Timeline of Lazarus Group activities

A quick glance at the timeline of the group's activities provides clues on the way they operate. Lazarus and its various subgroups will typically perform disruption and misdirection operations as part of their objectives. The group is fairly versatile as well, as they use a wide variety of tools and tactics to perform their attacks. Here are some examples of the group's objectives, tools, and procedures:

Notable Tactics of Lazarus

Disruption

The disruptive operations performed by Lazarus involve DDOS attacks and Wipers with time-based triggers. These include KILLMBR with a hard-coded wiping date, and QDDOS, which has duration date that wipes data ten days after infection. DESTOVER, a backdoor equipped with wiping capabilities, is another example.

Misdirection

Lazarus also included misdirection on some of their campaigns. Some operations were disguised as hacktivist activities, with groups such as "GOP," "WhoAmI," and "New Romanic Army" claiming responsibility for these alleged hacktivism attacks. They also tried to emulate the modus operandi of hacktivists by defacing web pages and leaking information.

Lazarus also plants false flags inside their tools as another misdirection technique. One example is the KLIPOD backdoor, which uses Romanized Russian words for its backdoor commands. While it is possible that Lazarus has members from different countries, the

Romanized Russian words do not appear to be written by a native speaker, and arguably used for misdirection.

While the objectives of these attacks vary from sabotage to financial gain, Lazarus did put some effort to misdirect attribution efforts towards other entities.

Protectors

Lazarus makes use of commercially available protectors for its tools. However, during their actual attacks, we have seen them deploy both protected and unprotected versions of their tools on the same target:

Anti-Forensics

Lazarus also employed some anti-forensics techniques in their operations, which include:

- **Separation of components:** In the later years of Lazarus operations, particularly operations related to the Bluenoroff subgroup, they made use of component separation for their malware
- **Command line tools:** Lazarus, again via Bluenoroff, makes use of command line backdoors and installers. Aside from separating the components, they also require specific arguments for execution. The installer of the Nestegg framework, for example, requires a password as an argument along with other switches. Their backdoor KLIPOD, on the other hand, receives its C2 server as a command line argument.
- **Disk Wiping**: Lazarus previously used wipers for disruption and sabotage. In later years, wiper samples in various forms can still be seen in their operations, although there are no reports of it being used. In particular, DESTOVER samples were seen in some of Bluenoroff operations, but no actual wiping occurred or was reported. In addition, command line forms of wiper tools were also recovered. These wipers may have been designed to wipe traces of the attacker's activities after the campaign has been completed, to leave as little evidence as possible.
- **Prefetch, event logs, and MFT record wipers**: In an effort to cover their tracks, Lazarus later made use of tools that can delete evidence. These include prefetch deletion, event logs deletion which support various OS versions, and MFT record wiping.

Defending against threats posed by Lazarus and other similar attacks:

The Lazarus Group—and any kind of targeted attack—is dangerous because of the wide variety of tools at their disposal and the different tactics they use depending on their targets and their objectives. This means that an organization's security and IT professionals must ensure that every corner of their network infrastructure is secure from different kinds of attacks. This includes ensuring that all machines connected to the network are always

updated with the latest security patches to minimize vulnerability exploitation. As information theft is also a prime objective of targeted attacks, protecting data from any possible breach should also be top priority.

Organizations can also look into multilayered security solutions such as Trend Micro™ Deep Discovery™, which provides real-time protection against targeted attacks. It can detect targeted attacks anywhere in the network. It features smart XGen™ technology that utilizes a blend of cross-generational techniques for applying the right technology at the right time, resulting in the highest detection rate possible. Trend Micro™ Office Scan™ protects the organization's users and corporate information by providing multiple layers of XGen™ security protection. It includes a comprehensive list of features such as machine learning, behavioral analysis, exploit protection, advanced ransomware protection, application whitelisting, sandbox integration, and more.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Cybercrime