9 Infamous APT Groups: Fast Fact Trading Cards

By Rob Sobers Updated: 3/29/2020

Advanced Persistent Threat (APT) groups are widely classified as organizations that lead, "attacks on a country's information assets of national security or strategic economic importance through either cyberespionage or cybersabotage." They are elusive, eminent and effective at what they do: wreaking havoc on their targets.

APTs don't just target enemy nations. Large corporations are also prime targets for certain APT groups, and it's absolutely crucial to catch APT operations before they can breach your perimeter. Once inside they deploy a wide range of methods to steal valuable information for internal intelligence, either to receive ransoms or for general sabotage (like shutting down enemy power grids).

Get the Free Pen Testing Active Directory Environments EBook

"This really opened my eyes to AD security in a way defensive work never did."

MITRE ATT&CK has 94 different groups logged as APT operations. These groups span across the world and include largely-funded government-backed groups as well as rag-tag teams of rogues who make a huge dent in the cybersecurity world.

Interested in the white hat hacking profession or working in cyber defense? Check out our free security training courses.

How Long Have We Been Naming APTs?

The date of the first instance of an APT group is up for debate just like the date of the first computer virus.

The term "Advanced Persistent Threat" was coined by the US Air Force in the early 2000s, but these groups have likely been operating since governments have been using digital operations.

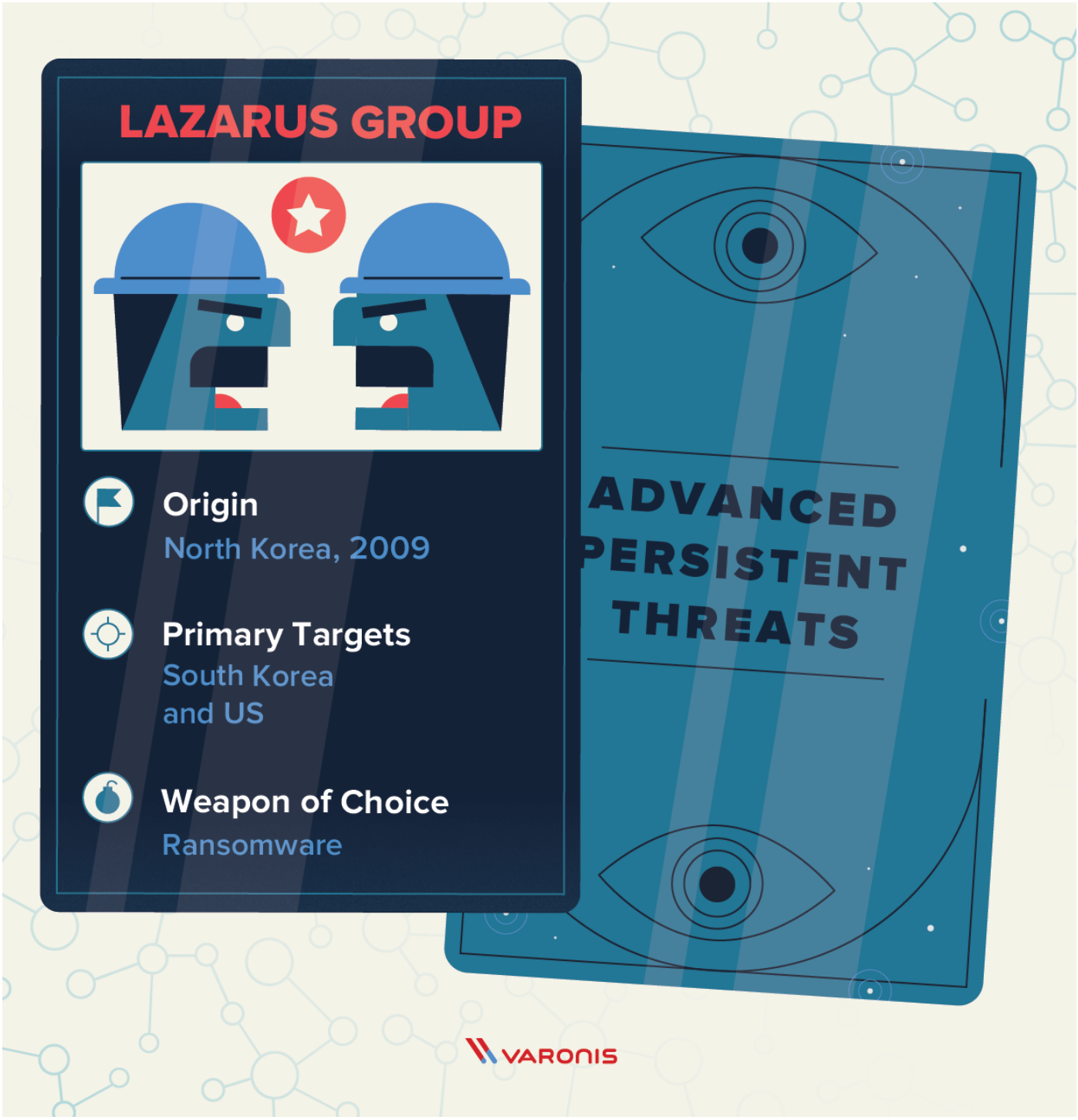
APT groups have been giving themselves cryptic monikers for as long as they've been operating. Sometimes others will name them, create spin-offs of the original name or additional nicknames will arise through the communities who follow them. It is said that many groups adopt the animal in their name based on the country they operate from (for example, Russia's calling card is a bear).

9 Prominent APT Group Trading Cards

Below we've grabbed some of the most prominent APT groups (listed in no particular order) and compiled stats to produce these APT "trading cards." Included on the APT trading cards are the group name, emblem interpretation, country or region of origin, if they are state-sponsored, their mode of operation (MO), targets and weapons of choice. Most of the labeled origins are suspected origins, not confirmed.

It's important to note that Varonis doesn't support or condone malicious cyber practices – this piece is strictly for educational purposes. Many of the groups below are government-sanctioned or funded, so one person's cybersecurity nightmare is another person's tax dollars at work — pretty strange to think about, right?

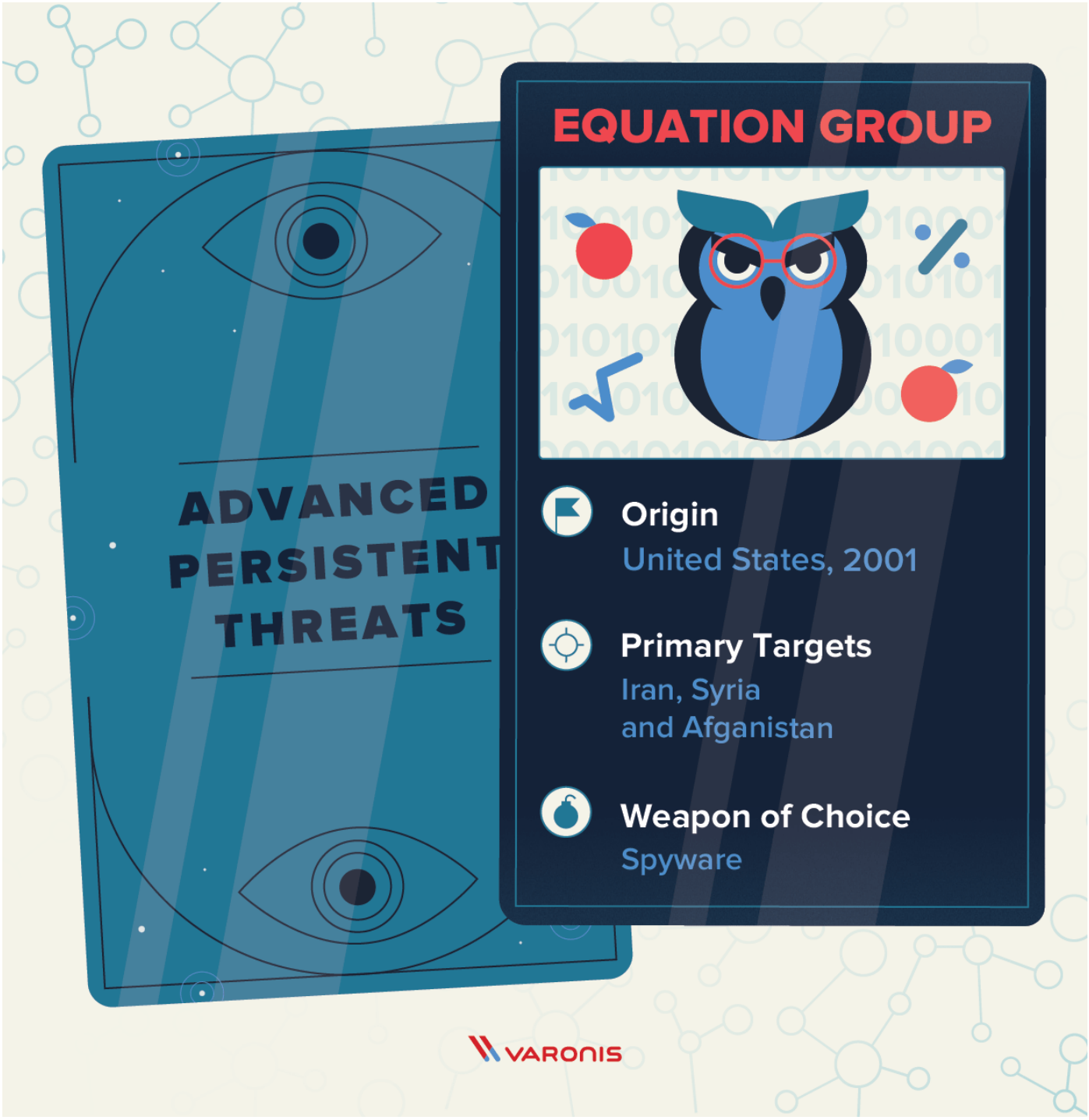
Lazarus Group



Lazarus Group has been tied to the North Korean government's Reconnaissance General Bureau (RGB). One of the attacks that they are best known for was the retaliatory attack on Sony in 2014 for producing a movie that painted their leader, Kim Jong-un, in an unflattering manner. The group and its members were sanctioned by the US for their activity.

- Origin: North Korea
- Established: 2009
- Primary Targets: South Korea, United States,
- Weapon of Choice: Ransomware (WannaCry, MimiKatz)

Equation Group



The Equation Group (also known as Shadow Brokers) is potentially connected to the US National Security Agency (NSA) or members of the NSA. A notable attack they're likely tied to took place 2010 and targeted Iran's nuclear program.

- Origin: United States

- Established: 2001
- Primary Targets: Iran, Syria, Afghanistan, Mali governments
- Weapon of Choice: Zero-day exploits, Spyware

Fancy Bear (APT 28)

Fancy Bear engages in political chaos and threats and is probably best known for their interference with Hilary Clinton's 2016 election campaign. While Russia hasn't taken responsibility for this group, the U.S. Department of Justice connected the group to Russian intelligence in a 2018 indictment.

- Origin: Russia
- Established: 2004
- Primary Targets: United States and Democratic National Committee (DNC), Germany
- Weapon of Choice: Spear-phishing, Mimikatz, Coreshell

Machete

Machete is a South American group that has been extremely hard to track. Since a lot of the entities they target are from Venezuela, they are likely based there. They use advanced phishing tactics to gain access and steal large amounts of sensitive data.

- Origin: South America

- Established: 2010
- Primary Targets: Venezuelan military and Columbia, Nicaragua and Ecuador
- Weapon of Choice: Phishing

Elfin (APT 33)

This group known as Elfin or APT 33 has been tied to Iran. They seem to have an interest in targeting aerospace, aviation and energy entities in the US, Saudi Arabia and South Korea. Elfin has an affinity for malware and has created its own custom malware like Stonedrill.

- Origin: Iran
- Established: 2013
- Primary Targets: Saudi Arabia and US (Aerospace and energy)
- Weapon of Choice: Shamoon, Mimikatz, PowerSploit and spyware

Mythic Leopard (APT 36)

Mythic Leopard has been linked to Pakistan and mainly focuses its resources on hacking and spear-phishing Indian government entities. The driving force behind these attacks is espionage to gain intelligence from the Indian government, military and other private Indian sectors. Using spear-phishing emails, Mythic Leopard was able to infect targets using a malicious

Excel file.

- Origin: Pakistan
- Established: 2016
- Primary Targets: India and the Indian Army
- Weapon of Choice: Social engineering

Dynamite Panda (APT 18)

Dynamite Panda has been tied to China and mainly targets medical, manufacturing, government and tech organizations based in the United States. Dynamite Panda made headlines when they breached private HIPAA-protected data in 2014 and stole the data of 4.5 million patients.

- Origin: China

- Established: 2009
- Primary Targets: United States
- Weapon of choice: Trojan ransomware

Charming Kitten

Most of the attacks that Charming Kitten has deployed have been aimed at individual Iranians who work in activism, media and academics — while they've also targeted Israel, the US and the UK. Hoping to spy or recruit defectors, Charming Kitten conducted an elaborate three-year spying operation targeted at US political figures through fraudulent, "journalist" social media accounts.

- Origin: Iran
- Established: 2014
- Primary Targets: Iran, Israel, US and UK
- Weapon of Choice: Account access

OceanLotus (APT 32)

The Ocean Lotus group is said to be based out of Vietnam, and its targets include Vietnam and other Southeast Asian countries like Laos, Thailand, Cambodia and the Philippines as well as Australia, the US and Germany. One of the most recent attacks tied to this group is the Toyota data breach. They deploy malware and use zero-day exploitation tactics to breach their

targets.

- Origin: Vietnam
- Established: 2014
- Primary Targets: Southeast Asian countries
- Weapon of Choice: Malware

To save a collection of all the trading cards, click the download button below.

If you are running point on cybersecurity for a government entity you are at especially high risk for being targeted by an APT group. See Varonis' government security solutions to learn how they can help take the pressure off and help bolster your security procedures, improve detection and speed up response times.

Sources: MITRE ATT&CK | SBS Cyber