kaspersky BRING ON THE FUTURE

Governmental organizations and APTs

"An APT is like a thief who breaks into a high-end automobile with the goal of using the garage door opener to later break into the car owner's mansion." (from Reverse Deception: Organized Cyber Threat Counter-Exploitation, by Bodmer, Kilger, Carpenter, Jones).

Let's start by taking a fresh look at what the term APT really means. The term has become part of the furniture of our cybersecurity vocabulary that there's a risk that some of its true implications can be overlooked. We're going to break it down right here:

Advanced: This doesn't mean that every single weapon in the APT arsenal is advanced. Just as traditional espionage and sabotage toolkits range from common eavesdropping to drone surveillance, the same is true of APTs. Obviously, APTs frequently implement tools and techniques that are well ahead of the curve when it comes to anything a lone basement hacker could procure or develop, such as false flag attacks like Olympic Destroyer. However it is the breadth and wealth of the APT toolkit that makes it truly advanced – the ability to meet every possible obstacle with a technique designed to bypass it (or destroy it).

Persistent: Here we could make the distinction between a thief who strolls by an open window and burglarizes on the spur of the moment, and an organized crime group who targets (and maybe achieves) control of an entire city council. The first is opportunistic, and APTs are anything but. The second never takes their eyes off the end goal, even if it takes more time to come to fruition. Putting the hungry ambition of individual members aside, every single action the group takes is weighed against its value in achieving total control over the city council. Everything. From small bribes, right through to murder. And everything must be done with a degree of stealth to avoid discovery. Persistence of that level, and of the level exhibited by APT groups, cannot be achieved by a small, disorganized band of hoodlums or basement hackers.

Threat: APTs put the capital T in Threat. Any kind of simple malware is a threat, but so is a fly buzzing around your head when you're trying to concentrate it. The fly? You just swat it away, and you win. Not the APT. What makes APTs so threatening is the combination of 'advanced' and 'persistent.' To use legal language, you have the weapon, and you have intent. Skill and tenacity. APTs can represent an existential threat to the organizations they attack – destroying businesses (if only temporarily), and paralyzing governmental institutions, programs or parastatals. Where military espionage is the key goal of an APT attack, the existential threat can be to human beings themselves.

> On the broader level, the answer is actually that simple. But of course it's easy to attack a municipal authority, a specific ministry, a national utilities grid, a science laboratory, a bank, or other critical infrastructure, than to attack central government itself. If you can't assassinate your target, at least you can weaken them, with deliberate decisive moves, or perhaps even by persistent attrition.

The operational complexity and resources required to fuel an APT group means that these are usually (though not always) state-sponsored. And who are the targets?

Other states.

Here are some key trends that governmental organizations need to be aware of to build a safe future for their citizens:

1. Mercenaries (Hacking-as-a-Service)
Just because APT groups are usually state-sponsored, it doesn't mean that they don't also use the services of external providers. The problem of mercenaries is just as real in the cybercrime war as they are when it comes to 'boots on the ground.' In August of this year (2020) we reported on a new mercenary triumvirate. DeathStalker is a Hacking-as-a-Service group that gathers sensitive information using PowerShell back doors and dead drop resolves on public services (among other techniques). We suspect DeathStalker to be linked to the Janicab, Powersing and Evilnum groups. One of their targets was a diplomatic entity. The DeathStalker group doesn't extort money from its victims. It doesn't need to – they're already being paid.

2. Targeted Ransomware
In October of 2020, multiple US hospitals were hit by Ryuk, a targeted ransomware attack that led the CISA, FBI and Department of Health and Human Services to issue a joint advisory, describing "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."

3. Geographical diversification of targets
In 2020, we observed several APT threat actors target countries that had previously drawn less attention, particularly along the geopolitically critical trade routes between Asia and Europe. We saw various malware used by Chinese-speaking actors used against government targets in Kuwait, Ethiopia, Algeria, Myanmar and the Middle East. We also observed StrongPity deploying a new, improved version of their main implant called StrongPity4. In 2020 we found victims infected with StrongPity4 outside Turkey, located in the Middle East.

4. The abuse of personal information: from deep fakes to DNA leaks
Leaked/stolen personal information is being used more than ever before in up-close and personal attacks. Threat actors are less afraid than ever to engage in active ongoing communications with their victims, as part of their spear-phishing operations, in their efforts to compromise target systems. We have seen this, for example, in Lazarus's activities and in DeathStalker's efforts to pressure victims into enabling macros. Criminals have used AI software to mimic the voice of a senior executive, tricking a manager into transferring more than £240,000 into a bank account controlled by fraudsters; and governments and law enforcement agencies have used facial recognition software for surveillance.

5. A further change of focus towards mobile attacks
This is apparent from the reports we have published this year. From year to year we have seen more and more APT actors develop tools to target mobile devices. Threat actors this year included OceanLotus, the threat actor behind TwoSail Junk, as well as Transparent Tribe, OrigamiElephant and many others.

So what can governmental organizations do about it?

The first step is to understand that even the most highly IT-matured governmental are not expected to tackle APT and APT-like attacks alone. It's a global problem, constantly shifting across regions and sectors, and a team would need at least 48 hours in the day to carry out the research and response tasks necessary for defending an organization against such a growing and shifting threat.

We encourage all of our IT-matured governmental customers to ensure that they diligently address what we see as the three pillars of any successful anti-APT security strategy. Namely, security teams must be:

- **Equipped:**
  Cybersecurity is one area of expertise where even a skilled worker can legitimately blame their tools. Protection from multivector attacks and APTs requires a unified consolidated platform that gives total visibility, eliminating obstructive siloes and preventing 'alert fatigue.'
- **Informed:**
  The existing advanced expertise of IT-matured organizations must never be taken for granted. After all, the cybercrime horizon is constantly shifting and expanding. Ongoing training and education from reliable cybersecurity research analysts is absolutely crucial.
- **Reinforced:**
  Should an APT be discovered, even the most advanced IT security analysts will need to resort to outside support for further contextual analysis and remediation. While APTs are usually highly targeted, they rarely target only one victim. External expertise can shed a multi-sector global light on the likely paths of an APT, and deliver actionable advice on the most decisive way to eliminate it from the system.

At Kaspersky we understand the challenges involved in defending against APTs and similar threats. That's why we've built a unified solution that fulfils the three pillars of a successful anti-APT security strategy. **Kaspersky Expert Security** empowers governmental organizations to make short work of sophisticated threats and APT-like attacks, meeting the challenges of stealth, persistence, siloes and talent head on. It's designed and built around Extended Detection and Response (XDR) platform and packed with features that augment the in-house superpowers of your IT security team, including comprehensive threat intelligence, expert guidance, training and emergency back-up 24/7.

Find out more about Kaspersky Expert Security

Kaspersky Expert Security

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/transparency

Proven. Transparent. Independent.