You have around 20 minutes to contain a Russian APT attack

Russian state hackers don't leave room for error in your cyber-security defenses.

By Catalin Cimpanu for Zero Day | February 19, 2019 -- 11:53 GMT (03:53 PST) |

Governments and private organizations have around 20 minutes to detect and contain a hack from Russian nation-state actors.

New statistics published today by US cyber-security firm CrowdStrike ranked threat groups based on their "breakout time."

"Breakout time" refers to the time a hacker group takes from gaining initial access to a victim's computer to moving laterally through its network. This includes the time the attacker spends scanning the local network and deploying exploits in order to escalate his access to other nearby computers.

The "breakout" metric is crucial for organizations, as this is the time they have to detect infections and isolate hacked computers before a simple intrusion turns into a compromise of its entire network.

According to data gathered from 2018 hack investigations, CrowdStrike says Russian hackers (which the company calls internally "Bears") have been the most prolific and efficient hacker groups last year, with an average breakout time of 18 minutes and 49 seconds.
They're followed by North Korean groups (Chollimas) with two hours and 20 minutes, Chinese hacker groups (Pandas) with four hours, Iranians (Kittens) with five hours and nine minutes, and cybercrime gangs (Spiders) with roughly nine hours and 42 minutes.

"The overall average breakout time that CrowdStrike observed in 2018 across all intrusions and threat actors was 4 hours 37 mins, a substantial increase from 1 hour and 58 minutes tracked in 2017," the CrowdStrike team said.
"While certainly not the only metric to judge sophistication by, this ranking by breakout time is an interesting way to evaluate the operational capabilities of major threat actors," they added.

The ability to break out of an initially compromised computer takes both skill and readily available hacking tools and exploits. It is only normal that Russian, North Korean, and Chinese groups rank high on this ranking, as they've been the most active cyber threat actors over the past decade, putting years of work into building advanced tools and honing their skills.

The "breakout time" metrics are included in the [2019 CrowdStrike Global Threat Report](https://www.crowdstrike.com/global-threat-report/) that the company published today. The report includes a summary of cyber operations carried out last year by both nation-state and cybercrime groups.

Some of the report's conclusions are:

- Nation-state adversaries were continuously active throughout 2018 --targeting dissidents, regional adversaries, and foreign powers to collect intelligence for decision-makers.
- Many countries used the media and diplomatic channels to claim they were curbing cyber-activities, but continued operations as normal.
- Sixty percent of all cyber-attacks involved a form of malware.
- China and North Korea accounted for almost half of all the nation-state attacks in 2018.
- Hacking supply chain companies instead of attacking targets directly has become a major trend.
- Iran and Russia have focused hacking efforts on telecom firms.
- Cybercrime groups are now increasingly using TTPs-for-hire (renting the services or tools provided by other groups, instead of creating their own).
- On the ransomware scene, criminal gangs adopted the tactic of "big game hunting," where they carry out targeted intrusion against large companies so they can extract bigger ransom demands at a time.
- CrowdStrike also observed increased collaborations between highly sophisticated criminal actors.
You have around 20 minutes to contain a Russian APT attack.

Image: CrowdStrike

https://www.zdnet.com/article/you-have-around-20-minutes-to-contain-a-russian-apt-attack/