RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: EFT-R03V

Two Weeks with a Russian Ransomware Cell

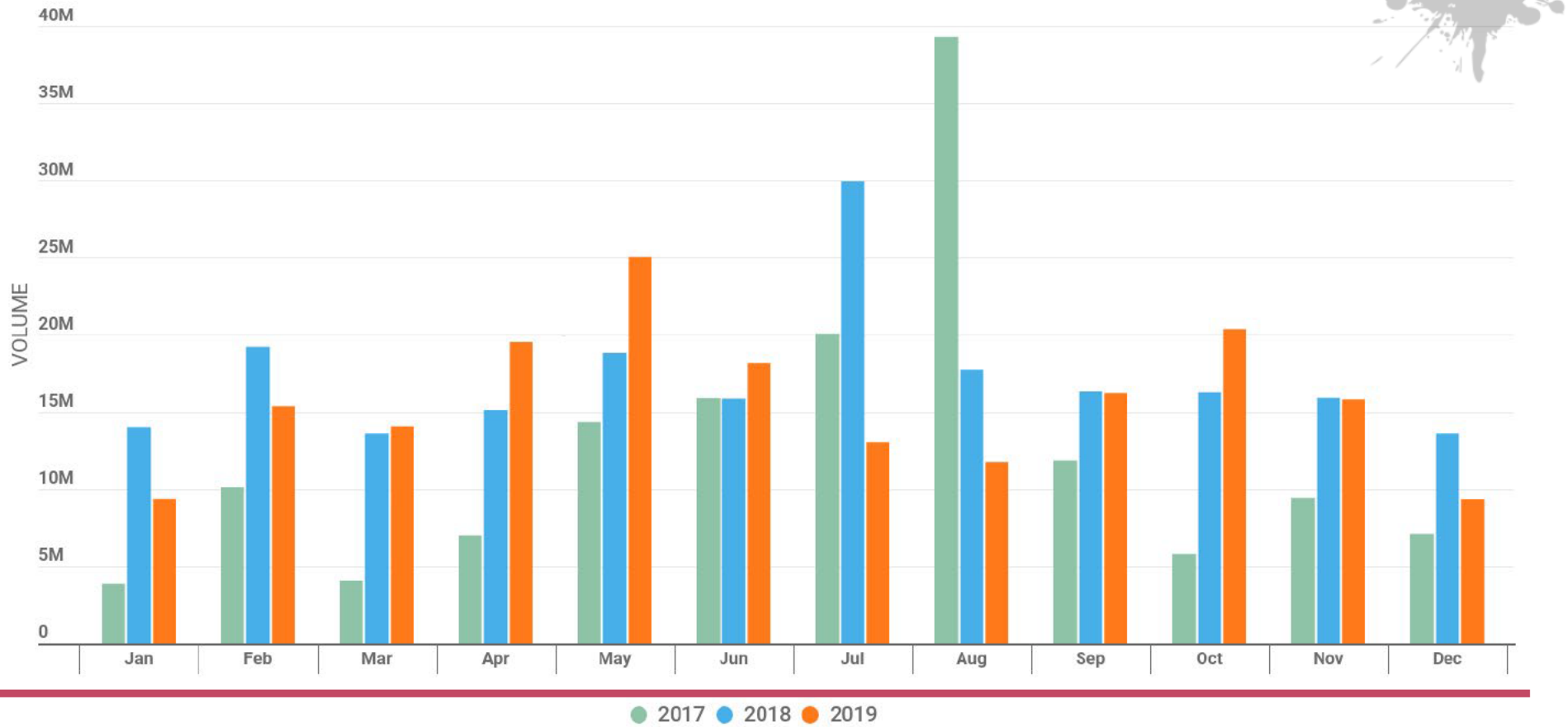
Brook Chelmo

Sr. Product Strategist
SonicWall
@BRChelmo

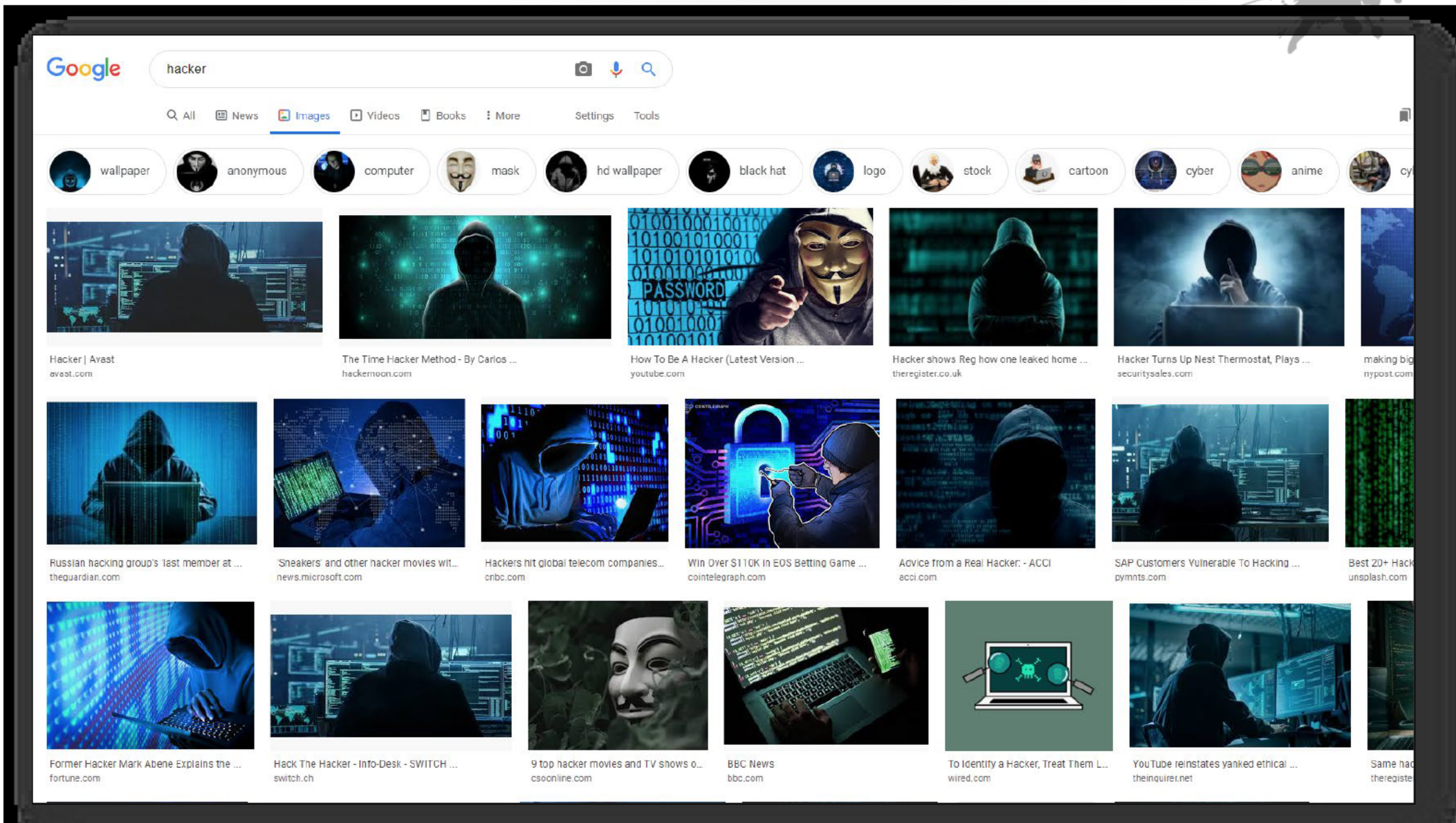
Targeting state, provincial & local governments

SonicWall recorded **187.9 million** in total ransomware volume for the year, a 6% drop from the record-breaking 2018 data.

Attacks systematically targeted governments and schools at all levels.



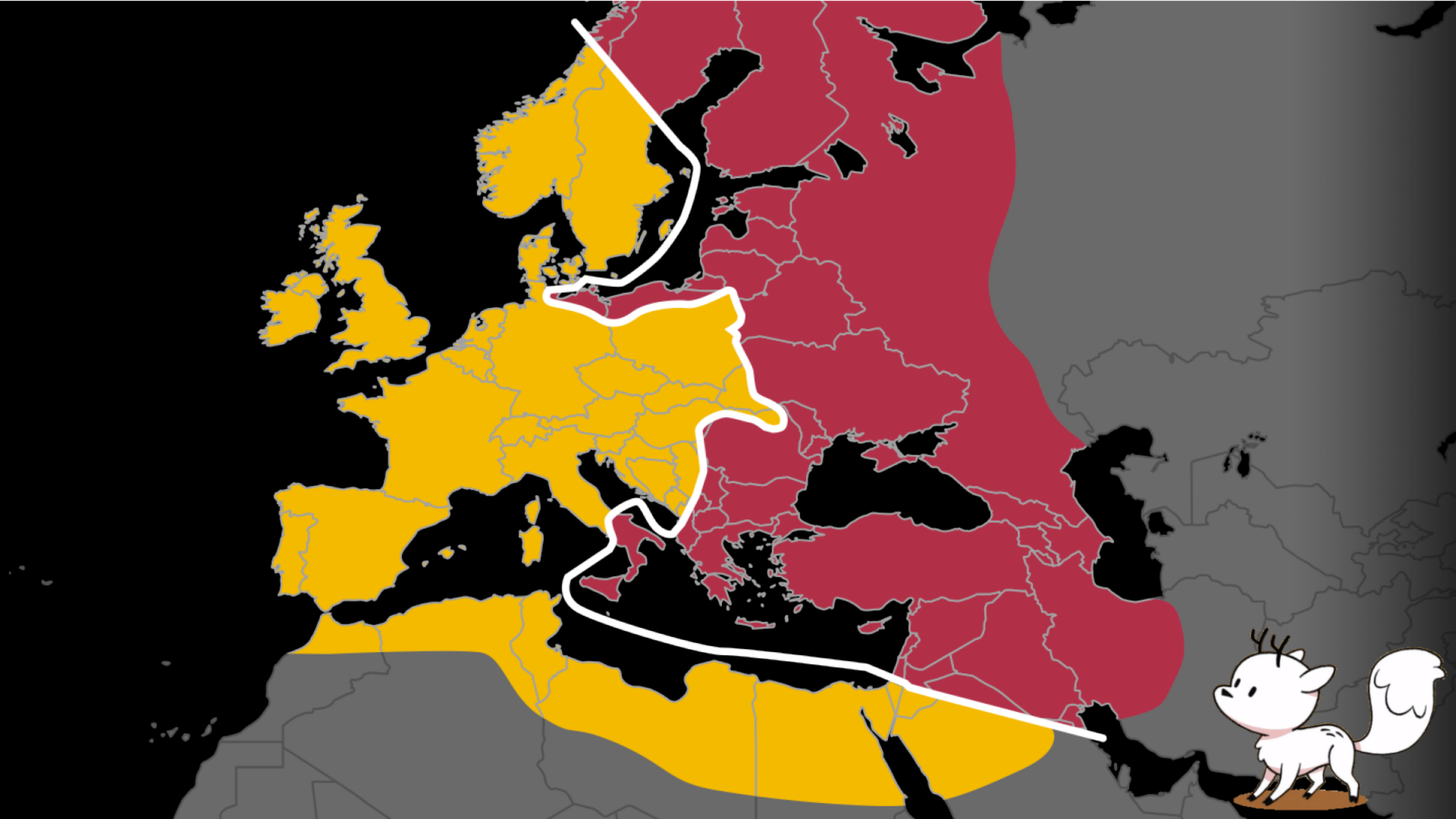
How do you visualize/perceive “hackers”



- Based in Russia
- Small group of young men
- Five ransomware families
- Developing new features
- Big plans
- They hate you

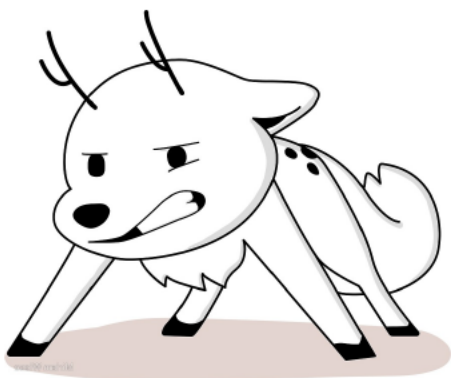
Types of attack missions

- Snoop – Stay invisible
  - Gain intelligence
  - Curiosity
- Exfiltrate – Stay invisible
  - Sell data on the black market
  - Hurt the host
- Extort – Get visible
  - Get paid now
  - Build a reputation



Twig's Intent

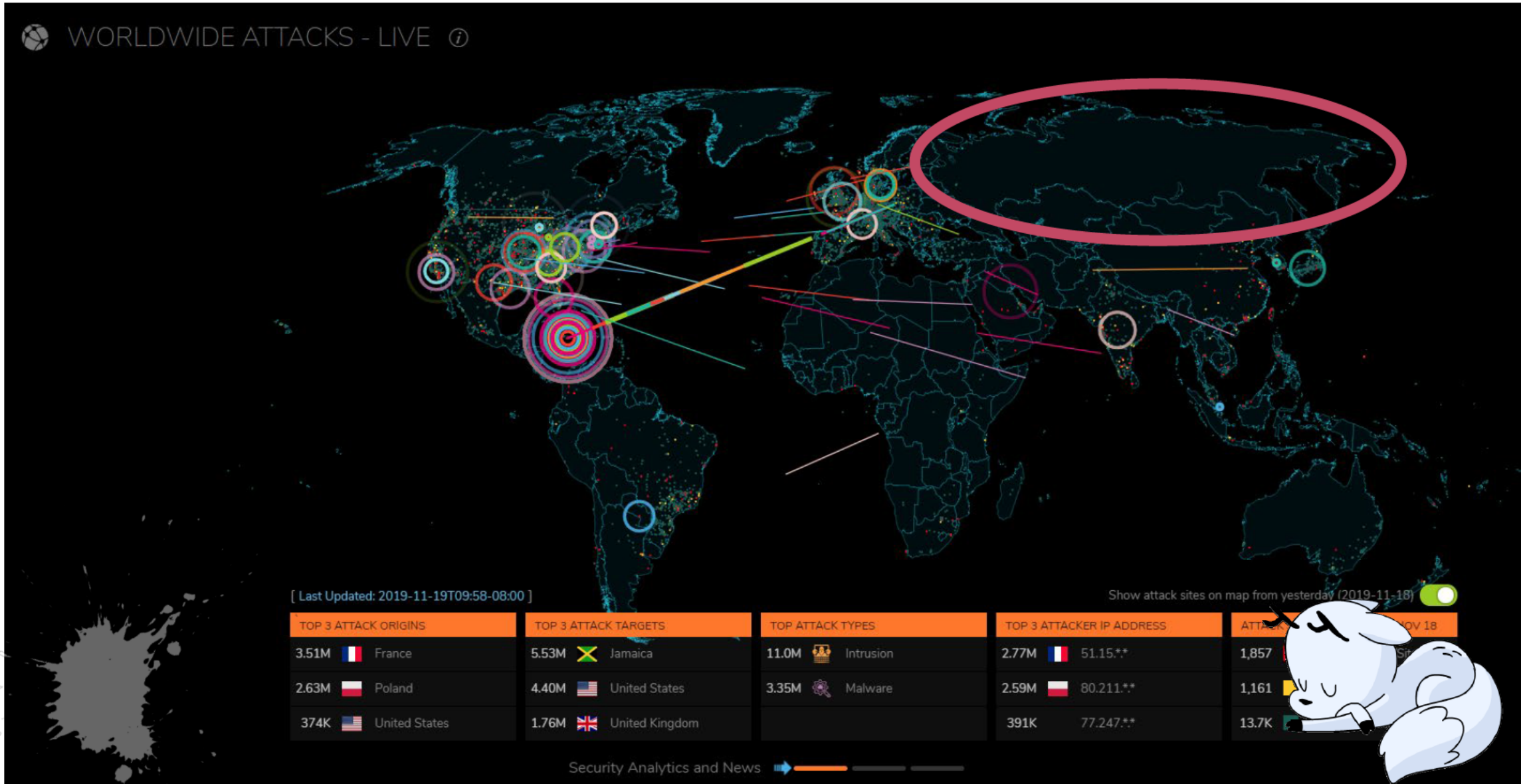
- Own source code
- Improve skills
- Build more feature
- Embarrass as many people as possible



How do they do it

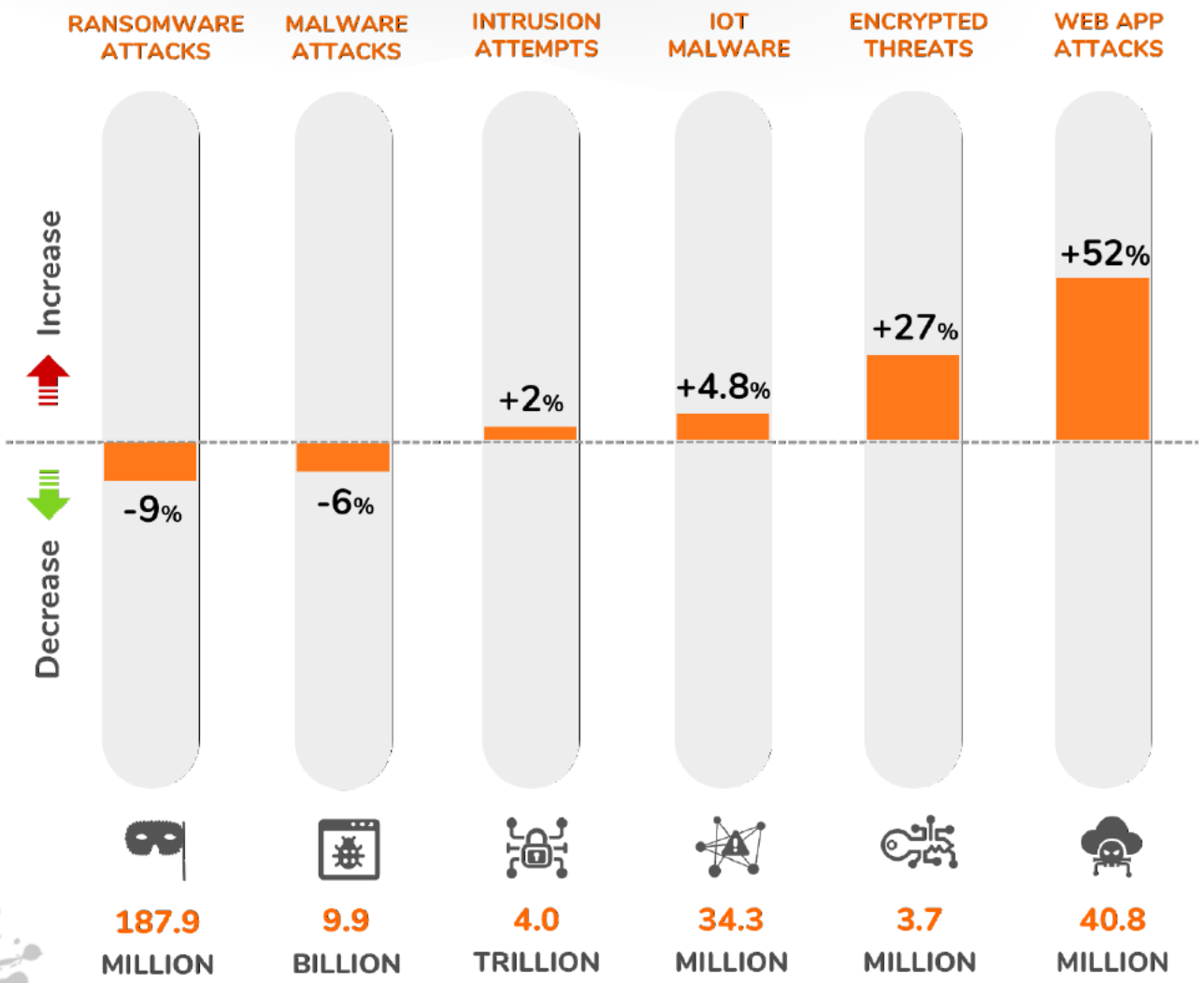
- Use Discord to ping servers
- Bulletproof C&C servers
- VPN/Encryption to hide intent
- PHP scripts
- Spear-phishing
- Attacking non-standard ports
- Common vulnerabilities
- Password-guessing
- Wash $BTC into $DASH

Why is Russia silent?



2019 global cyberattack trends

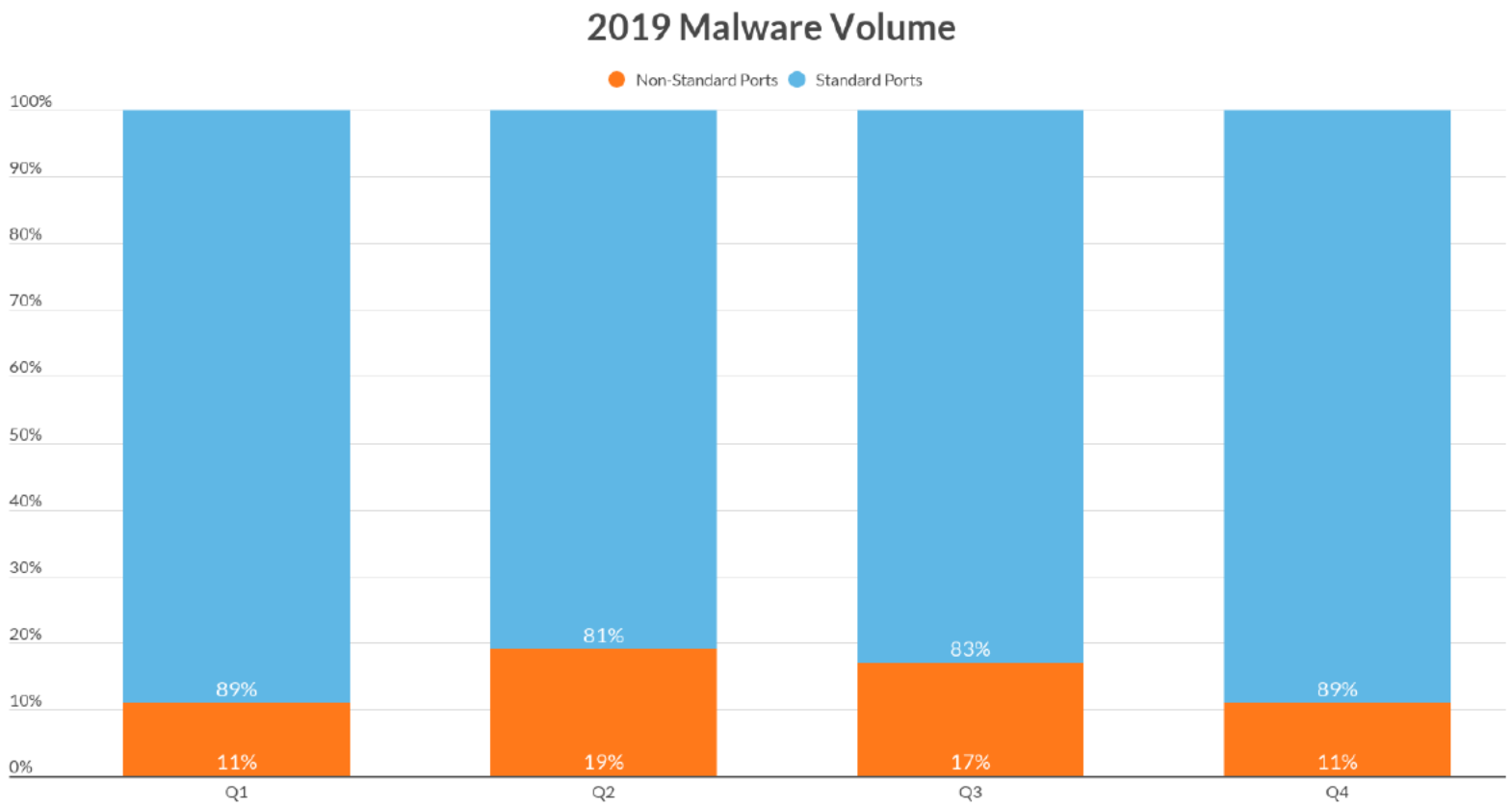
SonicWall Capture Labs threat researchers monitor and analyze real-time attack vectors throughout the year to help track dynamic threat behaviors and strategies.



2019 global cyberattack trends

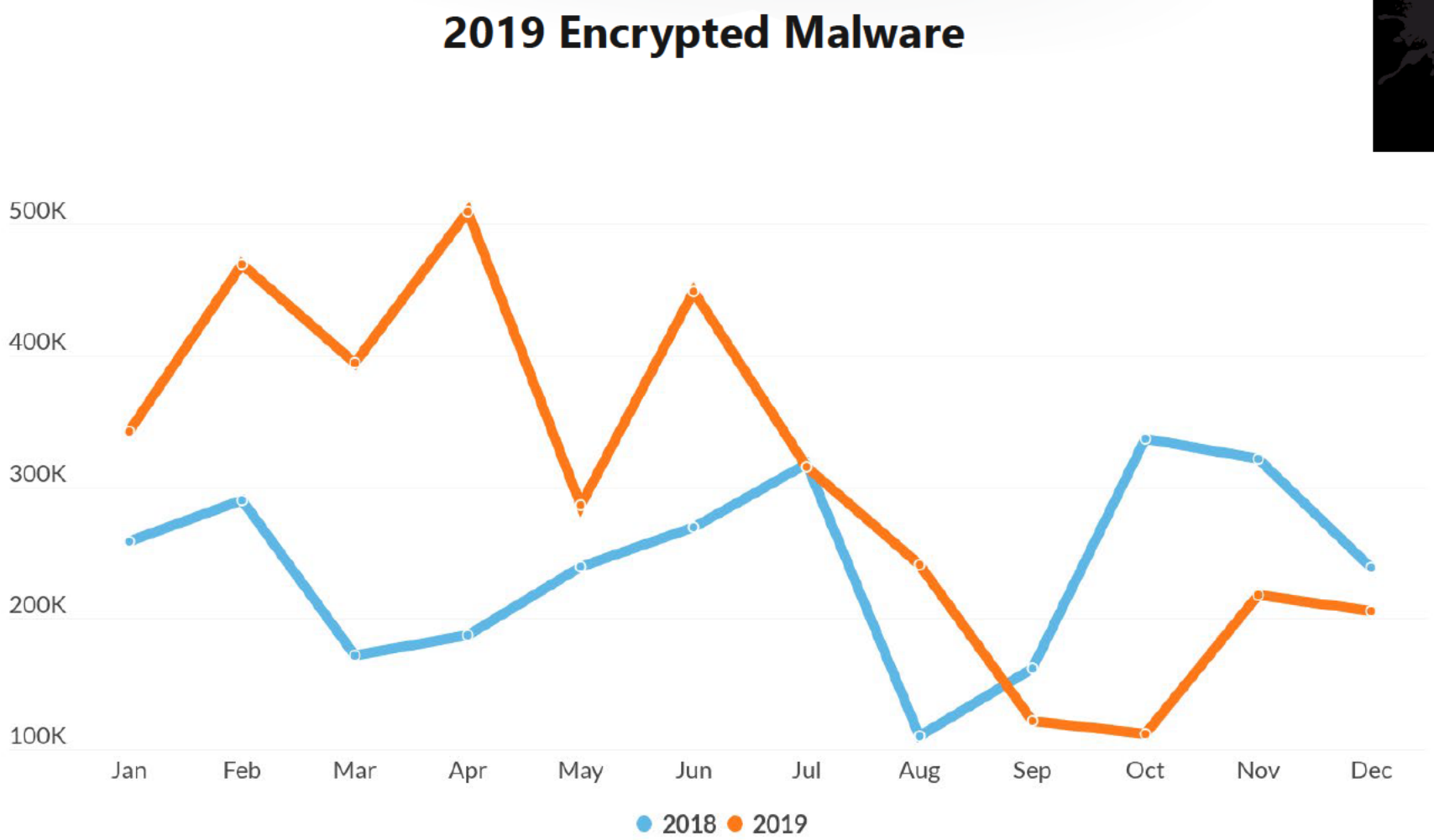
15% of all malware attacks coming over non-standard ports in 2019.

Traditional proxy-based firewalls aren't effective mitigating attacks over non-standard ports (for both encrypted and non-encrypted traffic).



Encrypted attacks growing consistently

SonicWall recorded **3.7 million malware attacks** sent over TLS/SSL traffic, a 27.3% year-over-year increase.



Twig's Advice

- Secure vulnerable ports
- Use proper passwords
- Write in a "real" programming language
- Employ the right people
- Watch for misconfigured firewalls

Twig's advice: proper passwords

- Require Multi-Factor Authentication
- Password length should be a minimum of 8 characters
- All special character (including space) should be allowed
- Eliminate knowledge-base authentication (e.g. what's your mother's maiden name?)
- Avoid personal information including name, important dates, pets, etc.
- Compare the prospective passwords against published compromised passwords

Twig's advice: write in a proper language

- Coding languages by open source security vulnerabilities:
  - C (47%)
  - PHP (17%)
  - Java (11%)
  - JavaScript (10%)
  - Phyton (5%)
  - C++ (5%)
  - Ruby (4%)

RSAConference2020 APJ

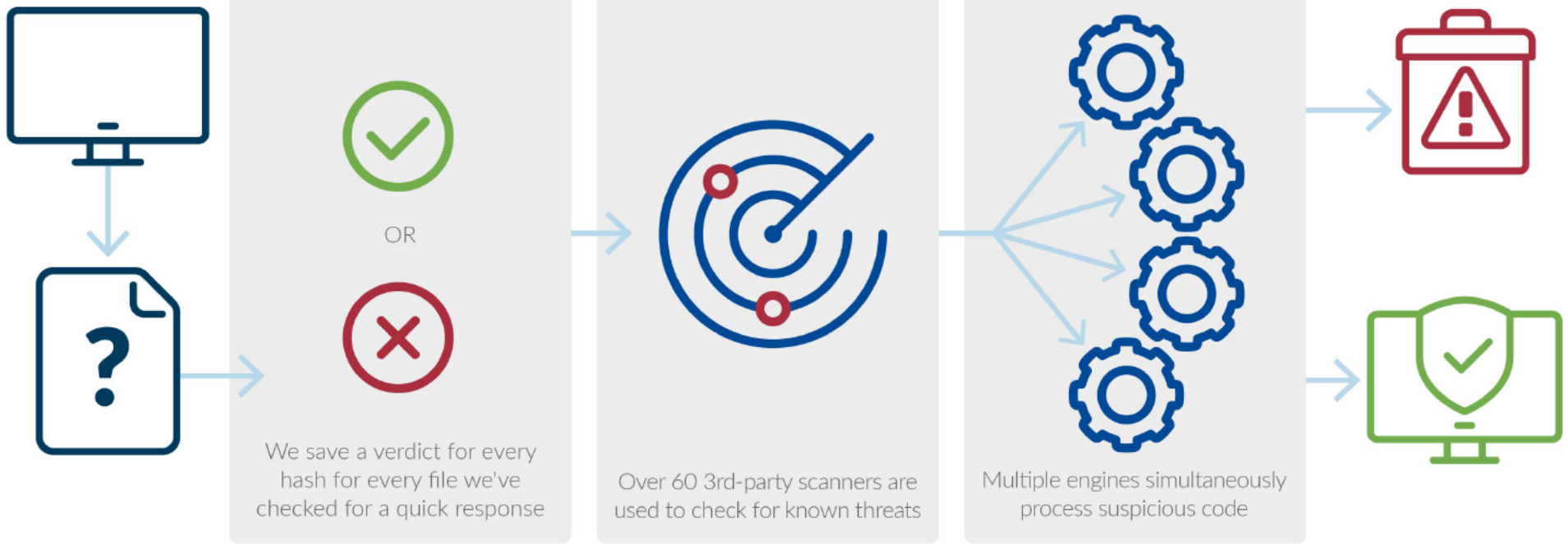
A Virtual Learning Experience

How do we stop ransomware authors?

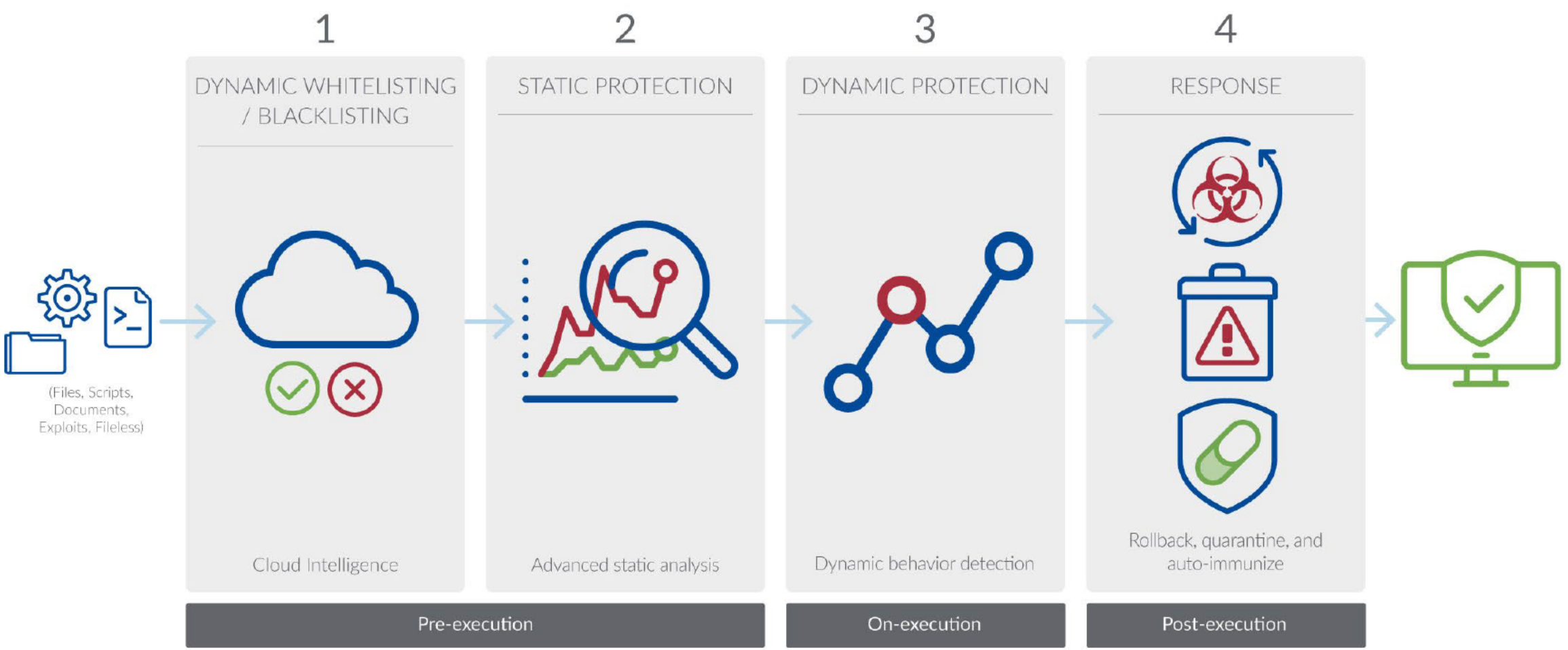
Technology for today's attacker

- 98% of attacks can be stopped with proper hygiene
- IT Admins/Execs have to list to their own advice
- Train employees on cyber attacks
- Perimeter defenses are still effective
- MITM encrypted traffic into networks
- Deploy sandboxing with memory-based analysis
- Email security is no longer a commodity-based solution set
- Heuristic anti-malware on endpoints is vital

How sandboxing should work



How endpoint security should work



What's next for Hildacrypt

- Bootlocker to prevent start up
- Runner to operate in memory
- Emulating SamSam

RSAConference2020 APJ

A Virtual Learning Experience

How do we stop Russian hackers a generation from now?

How to hire from the former Soviet Union

- C++ programmers = 2-3K/month
- Web developers = $1.2-2.2K/Mo.
- Never share full code base, host online with limited access
- On AWS use Team Foundation Server
- Always use project management software
- Ask for raw code at the end of a project

RSAConference2020 APJ

A Virtual Learning Experience