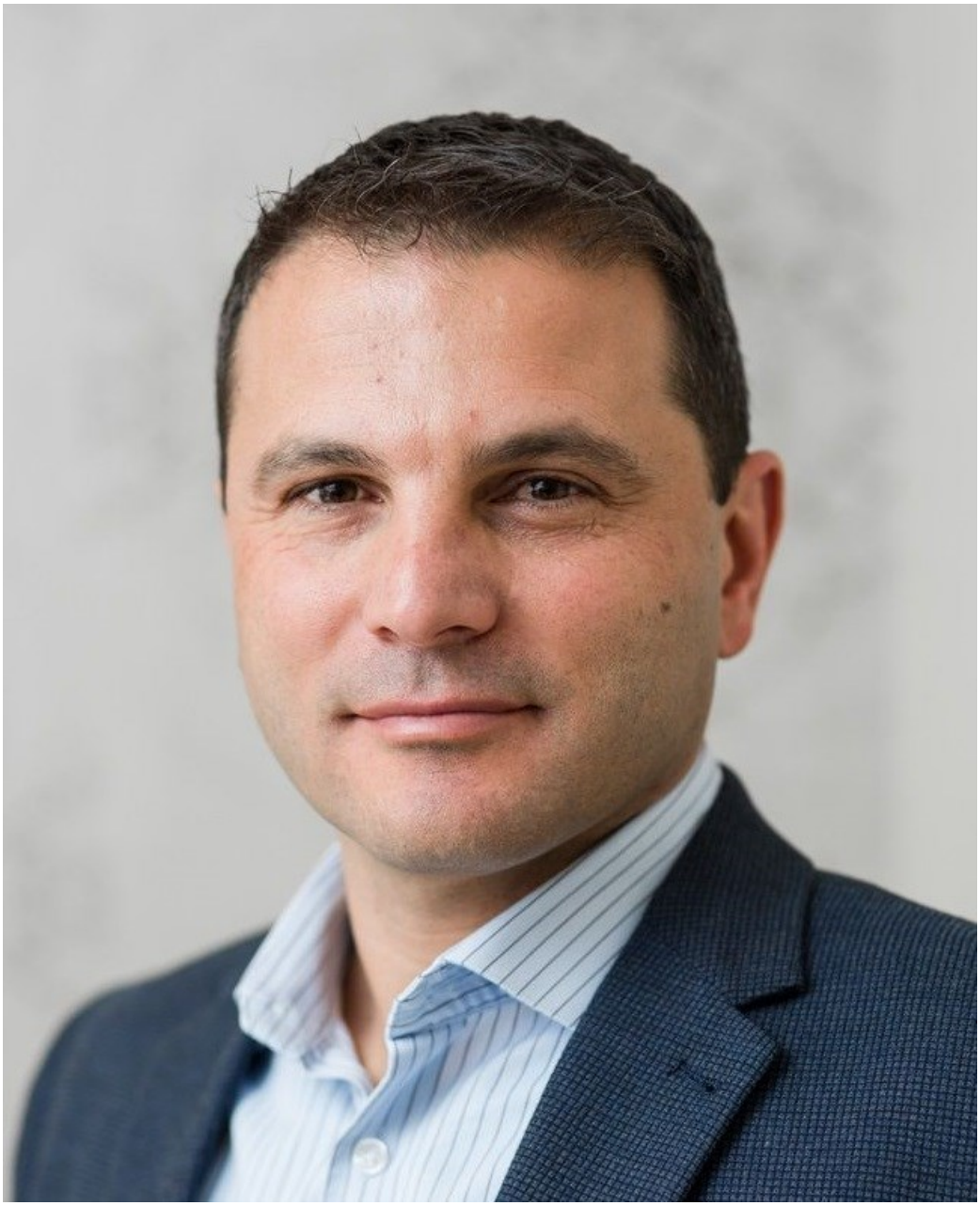
2018 attacks highlighted the need for advanced threat intelligence

By Doros Hadjizenonos

26 Mar 2019

In any situation where security or defence is the goal, lack of visibility into the techniques and tactics of your adversaries makes it nearly impossible to enact the right precautions. Time and time again, we have learned that it's not enough just to have a strategy.



Doros Hadjizenonos, Regional Director – SADC at Fortinet

Mapping, monitoring, and tracking the evolving threat landscape is fundamental to any security strategy. That’s why FortiGuard Labs is constantly evaluating and analysing the security incidents recorded by the millions of censors and security devices we have deployed in production environments around the globe.

This collected intelligence is comprised of billions of threat events every day. Using advanced AI solutions built around our advanced artificial neural network (ANN) and our global teams of highly skilled threat researchers, we are uniquely able to

provide the expertise and advanced threat intelligence cybersecurity teams need to deploy the correct security controls and processes to stay ahead of today's determined cybercrime community.

Organisations undergoing digital transformation are rapidly introducing a host of new devices and environments into their networks. This might include connected IoT devices, hybrid and multi-cloud environments, third-party applications, etc.

Because cyber threats often change and evolve in accordance with the expanding attack surface, subscribing to and leveraging threat research is an essential component of any organisation's security strategy.

Key Findings

Fortinet's Q4 Threat Landscape Index reveals 3 key findings:

1. IoT devices remain a focus

Cybercriminals are persistently targeting IoT devices. Despite the fact that IoT device exploit detections declined by 5% in Q4, 12 of the top global exploits continued to target IoT, with IP Cameras, printers, TVs, telephony equipment, and routers some of the most commonly targeted devices. Security cameras have been increasingly targeted, while cybercriminals continue to spend resources developing IoT-focused malwares and botnets.

VPNFilter was another IoT malware seen in 2018, which was able to steal website credentials, monitor traffic, and enabled crossover infection to other endpoint devices. The key takeaway here is that internet-facing devices will continue to be aggressively attacked, so security professionals must respond accordingly.

2. Increasingly evasive malware

Another trend seen in Q4, a microcosm of a larger trend for 2018, was increasingly agile and evasive malware that is able to detect vulnerabilities and evade detection with greater ease.

Shared opensource code has been a valuable resource for cybersecurity teams to test defences or develop new ones.

The challenge is that this malware, which is primarily designed for testing purposes, is publicly available and can readily be weaponised. Open source security tools can also be studied by cybercriminals in order to learn how to evade popular detection methods.

Additionally, throughout the course of 2018, cybercriminals adopted an agile development strategy, much like those being adopted by legitimate businesses, to more quickly release updates to malware in order to quickly counter anti-malware and updated security products.

3. Discovering zero-days exploits

2018 started off with the release of the Meltdown and Spectre, vulnerabilities found in most microprocessors, bringing with them the potential for disaster. A key reason that these vulnerabilities and zero-day threats like them are so dangerous is that security teams cannot see them coming.

This is another reason that threat research is so important to an effective security strategy – to ensure security teams are not entirely blindsided. To this end, FortiGuard Labs has honed in on research to discover zero-day exploits, leading the industry with over 650 such exploits and vulnerabilities being discovered over the last several years.

Need for threat intelligence services

If 2018 taught us anything, it's that as cybercriminals discover new and more profitable ways to target networks, cyberattacks can change in an instant. To address the unpredictability of this challenge, we have long advocated a learn, segment, protect approach to minimize the efficacy of these threats. This goes beyond just learning about your own network, but taking a global approach to threat analysis and then rethinking security in order to defend against threats that haven't even been created yet.

The biggest challenge many organisations face today is that they do not have the security infrastructure in place needed to conduct, consume, and implement the advanced threat research needed to alert them to new trends in cyberattacks or to zero-day vulnerabilities that must be patched.

These organisations need to invest in threat intelligence services to help them focus on the most pressing security matters of the day, along with new security controls and processes that enable them to share, correlate, and respond to threats in a coordinated fashion and at digital speeds.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...