HELP NET SECURITY

Featured news

- Will 2016 mark the end of the Advanced Persistent Threat?
- Guidelines for smart city technology adoption
- Anonymous goes after ISIS, aims to expose recruiters and sympathizers
- 9271 crucial vulnerabilities found in 185 firmware images of embedded devices
- Cyber crooks actively hijacking servers with unpatched vBulletin installations
- Unsafe password policies leave shoppers vulnerable
- Cross-device tracking via imperceptible audio beacons threatens user privacy
- BadBarcode: Poisoned barcodes can be used to take over systems
- Five hacks that will affect your life in 2016
- Phishers are targeting millions of DHL customers
- Bug in Android Gmail app allows effective email spoofing
- Information security innovation and the fast-paced threat landscape
- The appliance straightjacket and its effect on security
- Why governments need to take the lead in cybersecurity
- Ivan Ristic and SSL Labs: How one man changed the way we understand SSL

Will 2016 mark the end of the Advanced Persistent Threat?

Posted on 18 November 2015.

Advanced Persistent Threats (APTs) as we know them will cease to exist in 2016, replaced by deeper, embedded attacks that are harder to detect and trace back to the perpetrators, according to Kaspersky Lab experts.

In their predictions for 2016, experts reveal that while the ‘Threat’ will remain, the concept of ‘Advanced’ and ‘Persistent’ will disappear to reduce the traces left behind on an infected system. They will also rely more on off-the-shelf malware to minimize their initial investment.

Kaspersky Lab’s Predictions for 2016 are based on the expertise of the Global Research and Analysis Team, the company’s 42 top security experts, located all over the world. Each member contributes unique expertise and, in 2015 alone, their insight and intelligence resulted in detailed public reports on 12 APT actors, “speaking” different languages, including French, Arabic, Chinese, Russian, English, among others.

Kaspersky Lab experts anticipate that 2016 will see:

APTs lose letters, gain weight. There will be a dramatic change in how APTs are structured and operate:

- There will be a decreased emphasis on ‘persistence’, with a greater focus on memory-resident or fileless malware, reducing the traces left on an infected system and thereby avoiding detection.
- Rather than investing in bootkits, rootkits and custom malware that gets burned by research teams, researchers expect to see an increase in the re purposing of off-the-shelf malware. As the urge to demonstrate superior cyber-skills wears off, return on investment will rule much of the nation-state attacker’s decision-making and nothing beats low initial investment for maximizing ROI.

Thieves in the TV and/or crime in the coffee-maker. Ransomware will gain ground on banking Trojans and is expected to extend into new areas such as OS X.

New ways to make you pay. Alternative payment systems such as ApplePay and AndroidPay, as well as stock exchanges will become growing targets for financial cyber-attack.

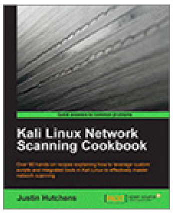
A leaked life. 2015 saw a rise in the number of DOXing, public shaming and extortion attacks, as everyone from haacktivists to nation-states embraced the strategic dumping of private pictures, information, customer lists, and code to shame their targets. Sadly, Kaspersky Lab expects this practice to continue to rise exponentially in 2016.

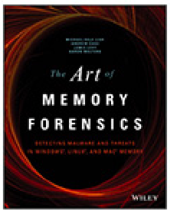
“2016 will see significant evolution in cyberespionage tradecraft, as sophisticated threat actors minimize investment by repurposing commercially available malware and become more adept at hiding their advanced tools, infrastructure, and identities by ditching persistence altogether,” said Juan Andrés Guerrero-Saade, Senior Security Expert, Global Research and Analysis Team, Kaspersky Lab.

“2016 will also see more players entering the world of cyber-crime. The profitability of cyber-attacks is indisputable and more people want a share of the spoils. As mercenaries enter the game, an elaborate outsourcing industry has risen to meet the demands for new malware and even entire operations. The latter gives rise to a new scheme of Access-as-a-Service, offering up access to already hacked targets to the highest bidder.” added Juan Andrés Guerrero-Saade.

APT | cybercrime | malware

Keep your business secure and compliant
GFI LanGuard™
Network security scanner and patch management





DON'T MISS
Tue, Nov 17th

- Anonymous goes after ISIS, aims to expose recruiters and sympathizers
- Cyber crooks actively hijacking unpatched vBulletin installations
- Five hacks that will affect your life in 2016
- Why governments need to take the lead in cybersecurity
- Ivan Ristic and SSL Labs: How one man changed the way we understand SSL

Back to TOP

HELP NET SECURITY

Search Help Net Security