# Kaspersky Lab's top cyber threat predictions for 2017

Kaspersky Lab's discovery in 2016 of an APT able to create new tools for each victim has effectively killed off 'Indicators of Compromise' as a reliable means of detecting infection, according to the company's *Threat Predictions for 2017* report.

©Brian Jackson via 123RF

The predictions are prepared annually by the company's Global Research and Analysis Team (GReAT) and are based on its wide-ranging insight and expertise. The list for 2017 includes the impact of bespoke and disposable tools, the growing use of misdirection in terms of attacker identity, the fragility of an indiscriminately Internet-connected world, and the use of cyberattacks as a weapon of information warfare.

## The decline of IoCs

Indicators of Compromise (IoCs) have long been an excellent way of sharing traits of known malware, allowing defenders to recognise an active infection. The discovery by GReAT of the ProjectSauron APT changed this. Analysis of the group revealed a bespoke malware platform where every feature was altered for each victim, rendering IoCs unreliable for detecting any other victim, unless accompanied by another measure, such as strong Yara rules.

## The rise of ephemeral infections

In 2017, Kaspersky Lab also expects to see the appearance of memory-resident malware that has no interest in surviving beyond the first reboot that will wipe the infection from the machine memory. Such malware, intended for general reconnaissance and the collection of credentials, is likely to be deployed in highly sensitive environments by stealthy attackers keen to avoid arousing suspicion or discovery.

"These are dramatic developments, but defenders will not be left helpless. We believe that it is time to push for the wider adoption of good Yara rules. These will allow researchers to scan far-and-wide across an enterprise, inspect and identify traits in binaries at rest, and scan memory for fragments of known attacks. Ephemeral infections highlight the need for proactive and sophisticated heuristics in advanced anti-malware solutions," said Juan Andrés Guerrero-Saade, senior security expert, Global Research and Analysis Team, Kaspersky Lab.

## Other top threat predictions for 2017

**Attribution will flounder among false flags**: As cyberattacks come to play a greater role in international relations, attribution will become a central issue in determining a political course of action – such as retaliation. The pursuit of attribution could result in the risk of more criminals dumping infrastructure or proprietary tools on the open market, or opting for open-source and commercial malware, not to mention the widespread use of misdirection (generally known as false flags) to muddy the waters of attribution.

**The rise of information warfare**: In 2016, the world started to take seriously the dumping of hacked information for aggressive purposes. Such attacks are likely to increase in 2017, and there is a risk that attackers will try to exploit people's willingness to accept such data as fact by manipulating or selectively disclosing information.

**Alongside this, a rise in vigilante hackers**: Hacking and dumping data, allegedly for the greater good.

**Growing vulnerability to cyber-sabotage**: As critical infrastructure and manufacturing systems remain connected to the internet, often with little or no protection – the temptation to damage or disrupt them could prove overwhelming for cyberattackers, particularly those with advanced skills, and during times of rising geopolitical tension.

**Espionage goes mobile**: The company expects to see more espionage campaigns targeted primarily at mobile, benefiting from the fact that the security industry can struggle to gain full access to mobile operating systems for forensic analysis.

**The commodification of financial attacks**: Kaspersky Lab expects to see the 'commodification' of attacks along the lines of the 2016 SWIFT heists in 2016 – with specialised resources being offered for sale in underground forums or through as-a-service schemes.

**The compromise of payment systems**: As payment systems become increasingly popular and common, the company expects to see this matched by a greater criminal interest.

**The breakdown of 'trust' in ransomware**: Also anticipated is the continuing rise of ransomware, but with the unlikely trust relationship between the victim and their attacker – based on the assumption that payment will result in the return of data – damaged as a lesser grade of criminal decides to enter the space. This could be the turning point in people being prepared to pay up.

**Device integrity in an over-crowded internet**: As IoT-device manufacturers continue to pump out unsecured devices that cause wide-scale problems, there is a risk that vigilante hackers could take matters into their own hands and disable as many devices as possible.

**The criminal appeal of digital advertising**: Over the next year, we will see the kind of tracking and targeting tools increasingly used in advertising being used to monitor alleged activists and dissidents. Similarly, ad networks – which provide excellent target profiling through a combination of IPs, browser fingerprinting, browsing interest and login selectivity – will be used by advanced cyberespionage actors keen to precisely hit targets while protecting their latest toolkits.

The full text of the report is available on Securelist.