KASPERSKY lab

Reality vs Delusion: A Guide to the Modern Threat Landscape

www.kaspersky.com

#truecybersecurity

Reality vs Delusion: A Guide to the Modern Threat Landscape

The next generation of threats: is there such a thing?

The never-ending war between hackers and cybersecurity vendors is a fine illustration of the "survival of the fittest" principle. The leading developers of defensive solutions are dead serious in their resolution to stop attackers in their tracks – and, until recently, were demonstrating considerable success. But this sort of pressure has also been a great stimulus to hackers inventing new tricks, techniques and business models, just in order to stay in business.

This Darwinian burst of evolution has provoked an interesting bidirectional progression, one direction being towards simplicity and the other towards focused sophistication. The effect of both progressions is a growing complexity in the threat landscape. To succeed against this requires levels of inventiveness, resources and experience that only a few market participants, those who are truly worthy of the 'next gen security vendor' title, possess.

Does that mean that 'next generation threats' have now arrived and are now threatening (forgive the unintended pun) businesses and private users alike?

The answer is yes and no.

For IT security professionals, the answer is, naturally, **negative**.

There is no catastrophic leap in hacking techniques that would imbue the attackers with godlike power against any given security system. Some of them were tried many years ago – but somehow were only marginally successful, often due to the technological restrictions of the global IT environment at the time. Now, with the IT firmament shifting into the right position, they have suddenly flourished, giving attackers a considerable edge against many existing solutions.

Then again, some defensive systems are holding their ground much better than others, their vendors constantly watchful for their adversaries' latest tricks and deploying whole arsenals of brand-new countermeasures without their customers even being aware. For the customer, everything feels quite natural: no vendor wants the complications and costs of introducing some new technology with its own interface that forces customer usage patterns to change, if the same technology can be delivered silently and transparently, ensuring the Best Possible Outcome for the customer.

But.

But for the end user, in an evolving IT environment with more and more to lose, experiencing a sudden burst of pressure from the attackers' side can feel like a dragon dropping out of seemingly clear sky. After spending years in blissful ignorance, being hit only by occasional malware infestations, businesses are realizing that suddenly they've become cash cows for very active cybercriminal entrepreneurs – who have no intention of leaving them alone, ever. So, for them 'Next Gen threats' feel very real.

The TOP4 IT Security concerns for businesses globally are about direct threats[1]

So, when somebody asks: "Is there such a thing as next generation threats?"– the answer is never simple. These threats may be not new, but they are powerful, hard to block and definitely may require considerable skill and experience and dedication from the vendors providing protective solutions. And the depth and breadth of underlying threat intelligence is of the utmost importance here, seamlessly fused with the technologies running on both customers' and vendors' premises.

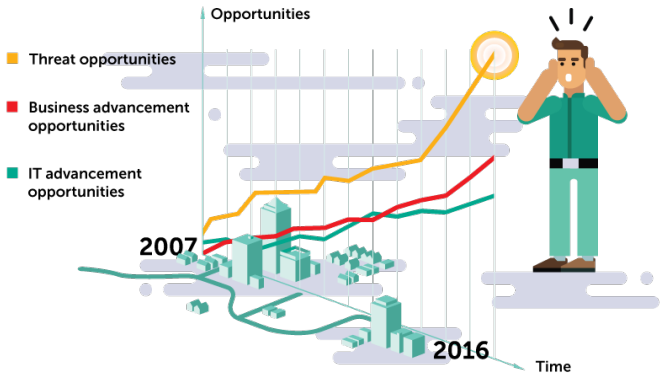
Some readers may well be quick to assume that the new Next Gen AVs are what's needed to battle this new onslaught. Unfortunately, as in most things, rushing to conclusions is a bad idea. One reason is that, given the diversity of these 'next gen' threats, protective approaches need to demonstrate at least equal diversity. Which means true multi-layered cybersecurity, capable of protecting from ALL threats, coming from every angle, rather than just those currently fancied by the most active attackers.

Unfortunately, the need for reliable protection from the broadest range of threats is all too often left out of the 'next gen' vendor's scope for the sake of simplicity and a lighter toll on system resources. As independent tests have proved, only too well.

In the meantime, the market leaders, such as Kaspersky Lab, are keenly aware of these threats' diversity and sophistication and usually offer *multiple*

1 Source: Global Corporate IT Security Risks Survey '2016 by B2B International & Kaspersky Lab

techniques to protect from each of them. We also recognize the critical importance of in-depth testing using the most lifelike scenarios. Participating regularly and enthusiastically in every possible independent test helps us perfect our protective layers, as well as deliver proof of trustworthiness of our claims.



This brings us back to what is truly 'next gen' about today's threats.

The Bidirectional Progress of Threats

The Trend Towards Simplicity

Taking cost efficiency as the leading principle, this trend is about simplicity in both development efforts and conducting the attacks themselves. For the developers, using off-the-shelf malware, tailoring it only marginally and relying on their victims' lack of proper security measures has generated a considerable success rate. So there really is no need to develop malware from scratch, when older software can be just as efficient. Simple!

The other area of simplification is about the marketing of malware offering convenient business models for the less skilled and patient cybercriminals to benefit from. Selling services rather than just trading in malware apps, or wrapping them into convenient interfaces and offering detailed FAQs and user support, has all resulted in a drastic expansion of the "hackers' bazaar", drawing in large numbers of 'script kiddie' hackers and other dilettantes. Naturally, the overall quantity of cyberattacks has increased as a result, greatly adding to the pressure experienced by businesses.

The Trend towards Sophistication

But all these new simplified business models don't mean a lack of technological progression in tools and techniques used by cyber attackers today: quite the opposite. Even 'script kiddies' can now obtain access to much more advanced malware than they were previously able to employ. And, when used by real specialists (and there are quite a few in the hacking community), the latest developments can really become something to be reckoned with.

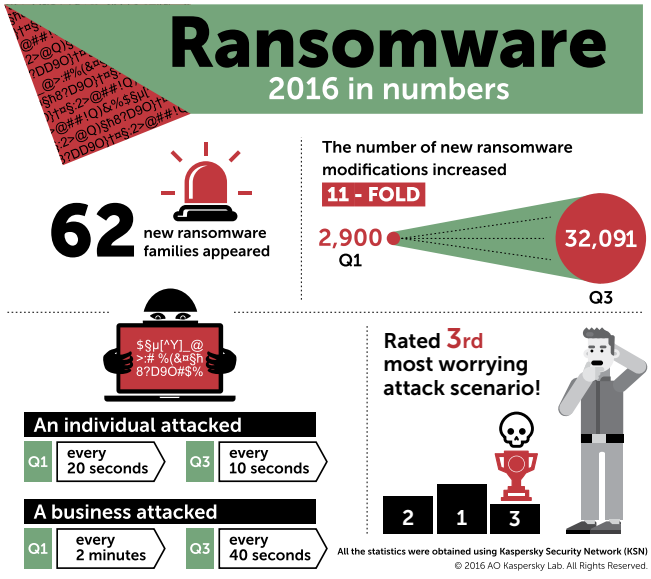
In addition, some techniques previously considered the prerogative of targeted attackers, are increasingly being adopted for mass infection campaigns (which can transform themselves into *something more targeted* at any time).

The Anonymity Veil

Perhaps one of the most important developments behind the recent tectonic shift in the threat landscape is increased anonymity. The emergence of Bitcoin and other crypto currencies has allowed for untraceable payments to be made, and anonymity mesh networks, such as Tor, offer new opportunities for the Black Hat hackers to communicate and trade both information and technologies without running great risk of exposure. While the most seasoned cybercriminals still form tight communities operating ' by invitation only', they nevertheless embrace the extra benefits provided by these newer techs – and some cybercriminal business models, such as ransomware (which was named the third most concerning ITsec problem globally[2]) have actually skyrocketed.

Ransomware

While not representing any particular technology, this phenomenon is nevertheless one of the most truly 'NextGen' threats we currently face. When



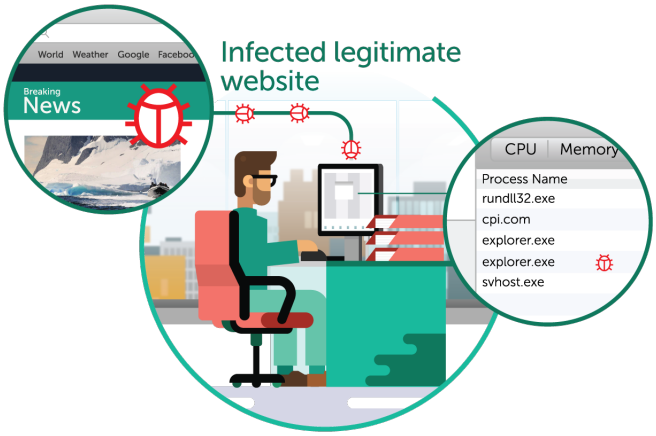
2 B2B International, May 2016

trying to describe what ransomware really is, what comes to mind is that it's a 'cybercriminal business model'. Technologically, it's backed not only by a wide range of attacking tools and techniques, but also by a number of anonymization measures. The emergence of cryptocurrencies and mesh networks (Tor, I2P etc.) allows criminals to receive payments while staying incognito, and this has triggered the current wave of ransomware, the biggest ever. If not addressed properly, ransomware can ruin your day in a most direct, destructive manner – with the chances of reversing its effects being extremely low. In the meantime, according to statistics, one of five victims who pay the ransom still can't decrypt their files – while supporting the culprits financially only stimulates the next wave of ransomware.

Different strains of ransomware can use different attack technologies and infection methods, so it's important to have multi-layered solutions equipped with specialized anti-ransomware technologies guarding your whole system. For example, our Kaspersky Endpoint Security for Business provides an anti-cryptor rollback system that would block the malware and then revert any files it already managed to encrypt to their previous state. Kaspersky Security for File Servers and Kaspersky Security for Storage feature another, complementary anti-cryptor engine that blocks encryption processes initiated through a different host on the network. And, for those using other vendors' solutions, the standalone (and free) Kaspersky Anti-Ransomware Tool can provide you with basic protection. The technology this free tool is based on is actually the same as is included in Kaspersky Endpoint Security – but there in our own solutions it's reinforced by many additional protection layers not included in the free application.

Memory-only malware

The fact that most malware comes in the convenient form of regular files fully justifies the importance of file-based detection. The lion's share of all the pre-execution detection takes place at this level. And, of course, this is not limited to simple narrow-sighted signatures: all kinds of heuristics, including structure and code-based analyses enable the detection even of previously unknown malware. But if malware operates outside the file system, this wealth of features suddenly becomes less useful. File artifacts can also provide a treasure trove of information for digital forensics. With all this in mind, attackers increasingly make use of 'memory-only' approaches, especially in targeted attacks. This can be achieved through different means, including the use of 'watering hole' infection techniques or by opening a (well-obfuscated in order to avoid premature detection) file attachment. The outcome is the same in each case: an injection is made into some already running process, and, from this moment on, the malware can function without ever touching the file system, including loading and launching extra modules and starting to move horizontally within the affected infrastructure.



To detect a plethora of advanced malware types, including memory-only malware, Kaspersky Endpoint Security features System Watcher, a technology based on the detection of suspicious app behavior, surveying activities within a given system. In this approach, it doesn't matter whether there's a file body behind the process under surveillance; any malicious activity will be blocked. System Watcher's detection principles are based on continuously running Machine Learning processes. They leverage extensive threat intelligence obtained through Kaspersky Security Network's Data Science-powered processing of globally obtained statistics.

Powershell: legal translator, illegal activities

Shell script files were long perceived as something harmless – though of course, when used creatively and with malicious intent, they are no such thing. But Powershell scripts are something else again – because they are truly powerful, offering an extremely wide range of opportunities for attackers. Downloading additional modules from the internet, running bodiless malware, performing the remote execution of arbitrary code on other machines in the network – and all this in the name of an inherently beneficial app, the Powershell interpreter, standard Windows equipment since Windows 7. Among the most notorious users of this particular technique are the infamous champion bank robbers from the Carbanak cybercriminal group.

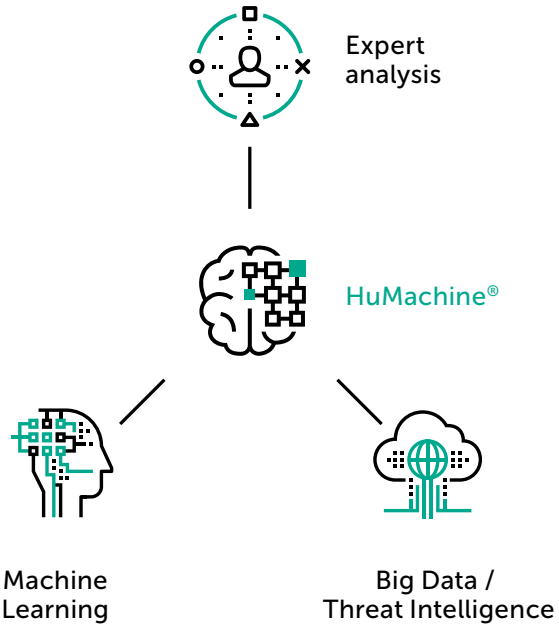
Kaspersky Lab is fully aware of this Powershell malware wave – as well as the use of regular shell scripts for malicious purposes. The strings passed to our engines are analyzed carefully, and execution is blocked should anything malicious be found.

The Mobile

Mobile phones and tablet computers are already the preferred means of accessing the internet. By the end of 2016, the number of smartphones used worldwide will have reached 2.1 billion: a rich crop for harvesting. Mobiles have already become deeply integrated into corporate business processes and data flows – but not always, unfortunately, into corporate cybersecurity infrastructures. Many factors, including rising geopolitical tensions, the growing popularity of mobile financial management and the sheer volume of sensitive data currently kept on these devices, all lead to the expectation that a burst of attacks against the mobile is on its way. The use of zero-day exploits for mobile cyberespionage is a reality, but even less sophisticated means can be very successful, especially when unexpected. One good example is a shameless malvertizing attack, when a banking Trojan was downloaded immediately after loading popular sites fitted with a particular ad network block containing a malicious JavaScript. The fact that the vast majority of Android smartphones are rootable without much hassle (including by fake/malicious apps), and some devices even arrive with malware pre-installed, means that system-level malware living beneath the user-controllable OS layer is not that uncommon.

Kaspersky Mobile Security for Business possesses a range of detection layers comparable to that of many desktop solutions; it's probably worth mentioning that some of them are powered by Machine Learning, leveraging the full power of our HuMachine intelligence. It also features additional powerful security layers such as Application Control. It is important that Mobile Security acts as a part of a single whole, together with Mobile Device Management and Mobile Application Management. Such an approach helps businesses create solid and especially secure mobility strategy.

Which means they are already understood, and the means of protection against them is available from leading vendors such as Kaspersky Lab, at this very moment. And, with our HuMachine approach – an efficient fusion of threat intelligence acquisition, data science amplified by machine learning processes and a world-famous team of experts – our customers can be sure of the Best Possible Outcome. However 'next gen' tomorrow's threats become, they will always be exposed and effectively countered by equally 'next gen' protection techniques. This is an important part of our vision of True Cybersecurity.



Conclusion

The list of techniques described above, though by no means comprehensive, is a fine illustration of levels of ingenuity, which only seasoned human professionals could hope to achieve. Perhaps they sow the seeds of increasing Fear, Uncertainty and Doubt in you, dear reader, so we need to remind you of several things right now, to dispel those fears.

First, once again, there's nothing fantastically new in these tricks. The most 'NextGen' development, in fact, is the means for untraceable communication and payment, such as Bitcoin and Tor-like networks. Even these have their roots in the more distant past, and are not inherently malicious themselves; double-edged blades used by cybercriminals for malicious purposes in the same way as many other legitimate tools.

Kaspersky Lab, Moscow, Russia **www.kaspersky.com**
All about Internet security: **www.securelist.com**
Find a partner near you: **www.kaspersky.com/buyoffline**

www.kaspersky.com