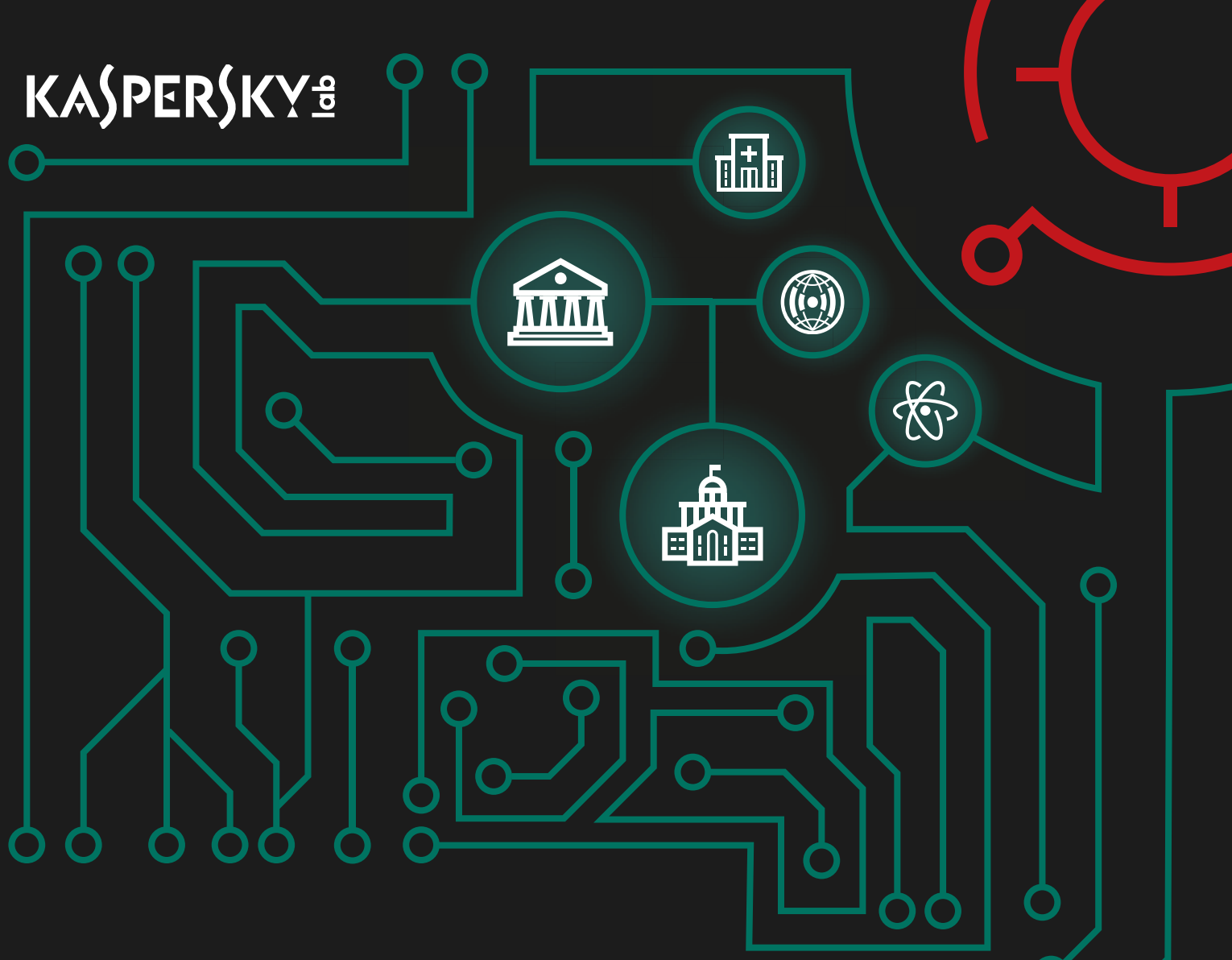
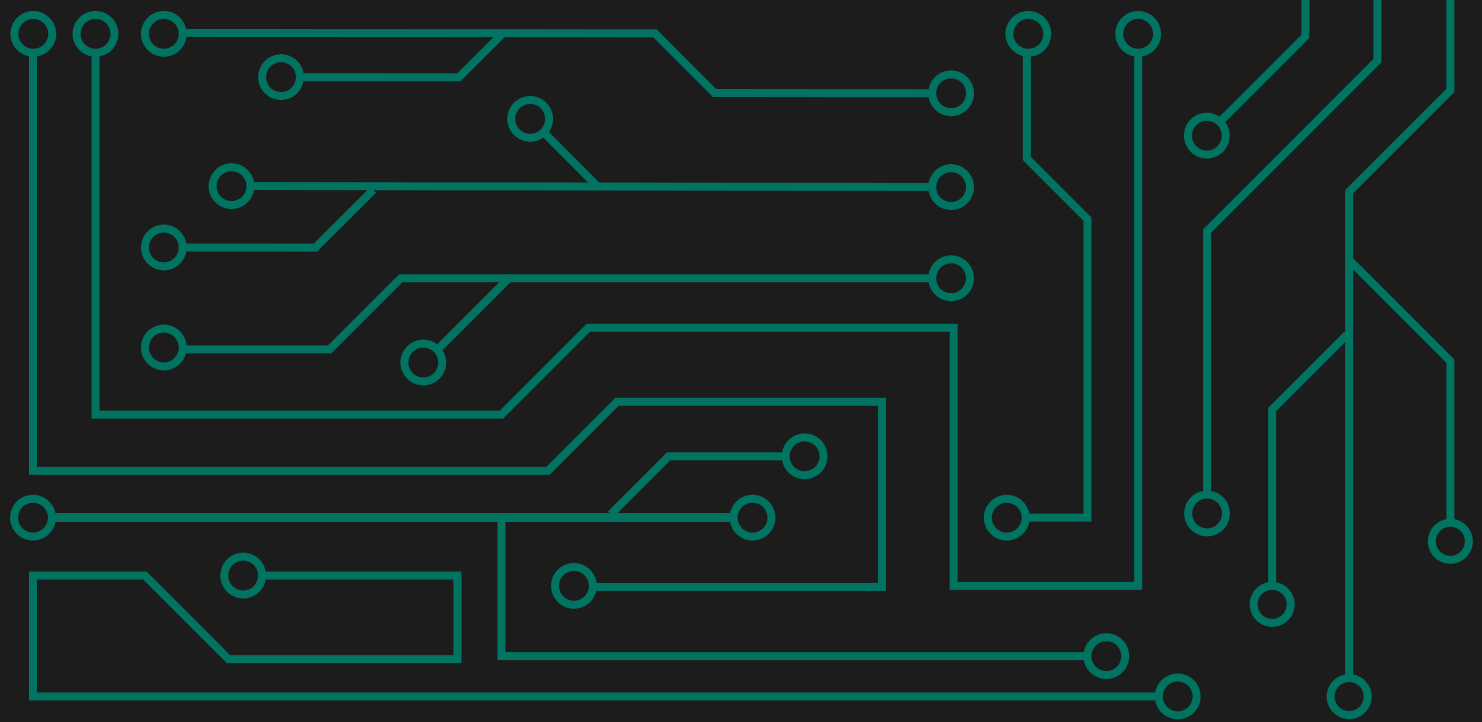
KASPERSKY lab



Kaspersky Security Bulletin:

STORY OF THE YEAR 2017



CONTENTS

Ransomware's new menace 4
- Introduction: what we learned in 2017 5
- The unanswered questions about WannaCry 6
- Leaked exploits powered many new waves of attacks 9
- Master keys released for several ransomware families 10
- The reappearance of Crysis 11
- RDP infections continue to grow 12
- Ransomware: a year in numbers 13
- Conclusion: what next for ransomware? 15
- The fight against ransomware continues 16

RANSOMWARE'S NEW MENACE

INTRODUCTION: WHAT WE LEARNED IN 2017

In 2017, the ransomware threat suddenly and spectacularly evolved. Three unprecedented outbreaks transformed the landscape for ransomware, probably forever. The attacks targeted businesses and used worms and recently leaked exploits to self-propagate, encrypting data and demanding a ransom they didn't really want. The perpetrators of these attacks are unlikely to be the common thieves usually lurking behind ransomware. At least one of the attacks carried flaws that suggest it may have been released too soon, another spread via compromised business software, two are related and the two biggest appear to have been designed for data destruction. The cost to victims of these three attacks is already running into hundreds of millions of dollars.

Welcome to ransomware in 2017 – the year global enterprises and industrial systems were added to the ever-growing list of victims, and targeted attackers started taking a serious interest in the threat. It was also a year of consistently high attack numbers, but limited innovation.

This short paper highlights some of the key moments.

THE MASSIVE OUTBREAKS THAT WERE NOT ALL THEY SEEMED

WannaCry

It all started on May 12, when the security community observed something it hadn't seen for almost a decade: a cyberattack with a worm that spread uncontrollably. On this occasion the worm was designed to install the WannaCry crypto-ransomware on infected machines.

The WannaCry epidemic affected hundreds of thousands of computers around the globe. To propagate, the worm used an exploit dubbed EternalBlue and a backdoor DoublePulsar, both of which had been made public by the Shadow Brokers group a month prior to the outbreak. The worm automatically targeted all computers sharing the same local subnet as the infected machine, as well as random IP ranges outside the local network – spreading it rapidly across the world.

To infect a machine, WannaCry exploited a vulnerability in the Windows implementation of the SMB protocol. Microsoft had released an update to fix this vulnerability back in March 2017, but the number of unpatched machines remained so high that this hardly hindered the propagation of WannaCry.

After infecting a machine and executing a routine to spread further, WannaCry encrypted some valuable files belonging to the victim and displayed a ransom note. Full decryption of the affected files was impossible without paying the ransom – although our analysts discovered several flaws in WannaCry's code that could allow some victims to restore some of their data without paying the ransom.

Impact of WannaCry

The attack was industry-agnostic, and victims were mainly organizations with networked systems. The ransomware also hit embedded systems. These often run on legacy OS and are therefore particularly vulnerable. Victims received a ransom demand to be paid in bitcoins. Reports suggests the ultimate number of victims could be as high as three-quarters of a million.

Car maker Renault had to close its largest factory in France and hospitals in the UK had to turn away patients. German transport giant Deutsche Bahn, Spain's Telefónica, the West Bengal power distribution company, FedEx, Hitachi and the Russian Interior Ministry were all hit, too. A month after the initial outbreak had been contained, WannaCry was still claiming victims, including Honda, which was forced to shut down one of its production facilities, and 55 speed cameras in Victoria, Australia.

The unanswered questions about WannaCry

As a devastating high profile attack targeting businesses, WannaCry was extremely successful. As a ransomware plot to make lots of money, it was a failure. Spreading via a worm is not advisable for a threat that is most lucrative when silently stalking the shadows. Estimates suggest it only made around $55,000 in bitcoin, hampered by its high visibility. The code was poor in places, and there are suggestions that it escaped into the wild before it was fully ready. There are also a number of indicators, including early code similarities that suggest the group behind WannaCry is the infamous Korean-speaking threat actor Lazarus.

The true purpose of the WannaCry attack may never be known – was it ransomware gone wrong or a deliberate destructive attack disguised as ransomware?

ExPetr

The second big attack came just six weeks later, on June 27. This was spread predominantly through a supply chain infection and targeted machines mainly in Ukraine, Russia and western Europe. The company's telemetry indicates that there were more than 5,000 attacked users. Victims received a 'ransom demand' of around $300, to be paid in bitcoins – although it turned out that even then they couldn't get their files back.

ExPetr was a complex attack, involving several vectors of compromise. These included modified EternalBlue (also used by WannaCry) and EternalRomance exploits and the DoublePulsar backdoor for propagation within the corporate network; compromised MeDoc accounting software, which distributed the malware through software updates; and a compromised news website for Ukraine's Bakhmut region that was used as a watering hole by the attackers.

What's more, ExPetr was capable of spreading even to properly patched machines in the same local network as the initially infected computer. To do that, it harvested credentials from the infected system by means of a Mimikatz-like tool and proceeded with its lateral movement by means of the PsExec or WMIC instruments.

The encrypting component of ExPetr operated on two levels: encrypting the victim's files with the AES-128 algorithm and then installing a modified bootloader taken from another malicious program – GoldenEye (the successor of the original Petya). This malicious bootloader encrypted the MFT, a critical data structure of the NTFS file system, and prevented further boot processes, asking for a ransom.

Impact of ExPetr

Victims of ExPetr included major organizations such as shipping ports, supermarkets, ad agencies and law firms: for example, Maersk, FedEx (TNT) and WPP. A month after the attack, TNT's deliveries were still affected, with SMB customers suffering most. Another victim, consumer goods giant Reckitt Benckiser, lost access to 15,000 laptops, 2,000 servers and 500 computer systems in the space of just 45 minutes when the attack hit – and expects the cost to the business to be over $130 million. Maersk announced a revenue loss of around $300 million due to the attack.

The unanswered questions about ExPetr

Kaspersky Lab experts have found similarities between ExPetr and early variants of BlackEnergy's KillDisk code – but the true motivation and purpose behind ExPetr also remain unknown.

BadRabbit

Then, in late October, another crypto-worm, BadRabbit, appeared. The initial infection started as a drive-by download served from a number of compromised websites and mimicking an update for Adobe Flash Player. When launched on a victim's computer, BadRabbit's worm component attempted to self-propagate using the EternalRomance exploit and to employ a lateral movement technique similar to the one utilized by ExPetr. Most of BadRabbit's targets were located in Russia, Ukraine, Turkey and Germany.

The ransomware component of BadRabbit encrypted the victim's files, followed by the whole disk partitions using modules of legitimate utility DiskCryptor. The analysis of the code of BadRabbit samples and techniques suggests there is a notable similarity between this malware and ExPetr. However, unlike ExPetr, BadRabbit does not appear to be a wiper, as its cryptographic scheme technically allows the threat actors to decrypt the victim's computer.

LEAKED EXPLOITS POWERED MANY NEW WAVES OF ATTACKS

The criminals behind the aforementioned ransomware outbreaks were not the only ones to use the code of exploits leaked by the Shadow Brokers to wreak havoc.

We have discovered some other not-so-notorious ransomware families that at some point used the same exploits. Among them are AES-NI (Trojan-Ransom.Win32.AecHu) and Uiwix (a variant of Trojan-Ransom.Win32.Cryptoff). These malware families are 'pure' ransomware in the sense that they do not contain any worm capabilities, i.e. cannot self-replicate, which is why they did not spread nearly as widely as WannaCry, for instance. However, the threat actors behind these malware families exploited the same vulnerabilities on victims' computers during the initial infections.

MASTER KEYS RELEASED FOR SEVERAL RANSOMWARE FAMILIES

Apart from the large-scale epidemics that shook the world, in Q2 2017 an interesting trend emerged: several criminal groups behind different ransomware cryptors concluded their activities and published the secret keys needed to decrypt victims' files.

Below is the list of families for which keys became public in Q2:

- Crysis (Trojan-Ransom.Win32.Crusis);
- AES-NI (Trojan-Ransom.Win32.AecHu);
- xdata (Trojan-Ransom.Win32.AecHu);
- Petya/Mischa/GoldenEye (Trojan-Ransom.Win32.Petr).

The Petya/Mischa/GoldenEye master key was released shortly after the outbreak of ExPetr and might have been an attempt by the original Petya authors to show that they were not the ones behind ExPetr.

THE REAPPEARANCE OF CRYSIS

Despite the fact that the Crysis ransomware appeared to die in May 2017 following the release of all the master keys, it didn't stay dead for long. In August, we started discovering numerous new samples of this ransomware and they turned out to be almost identical copies of the previously distributed samples, with only a few differences: they had new master public keys, new email addresses that victims were supposed to use to contact the criminals, and new extensions for the encrypted files. Everything else remained unchanged – even the timestamps in the PE headers. After thorough analysis of the old and new samples, our analysts concluded that most likely the new samples were created by binary patching the old ones using a hex editor. One reason for this might be that the criminals behind the new samples didn't possess the source code and simply reverse-engineered the ransomware to raise it from the dead and use it for their own ends.

RDP INFECTIONS CONTINUE TO GROW

In 2016, we noticed a new emerging trend among the most widespread ransomware. Instead of trying to trick the victim into launching a malicious executable or using exploit kits, the criminals turned to another infection vector. They were brute-forcing the RDP logins and passwords on machines that had RDP turned on and that were available for access from the Internet.

In 2017, this approach became one of the main propagation methods for several widespread families, such as Crysis, Purgen/GlobeImposter and Cryakl. This means that when securing a network, InfoSec specialists should keep this vector in mind and block RDP access from outside the corporate network.

RANSOMWARE: A YEAR IN NUMBERS

It is important not to read too much into the absolute numbers as they reflect changes in detection methodology as much as they do evolution of the landscape. Having said that, a few top line trends are worth noting:

- The level of innovation appears to be declining – in 2017, 38 new strains of encryption ransomware were deemed interesting and different enough to be designated as new 'families', compared to 62 in 2016. This could be due to the fact that the crypto-ransomware model is fairly limited and it is becoming progressively more difficult for malware developers to invent something new.

- There were many more modifications of new and existing ransomware detected in 2017: over 96,000 compared to 54,000 in 2016. The rise in modifications may reflect attempts by attackers to obfuscate their ransomware as security solutions get better at detecting them.

- The number of attacks as defined by hits against Kaspersky Lab customers remained fairly constant. In fact, the big spikes of 2016 have been replaced with a more consistent monthly spread. Overall, just under 950,000 unique users were attacked in 2017, compared to around 1.5 million in 2016. However, this data includes both encryptors and their downloaders; if you look at the numbers for encryptors only, the attack data for 2017 is similar to 2016. This makes sense if you consider that many attackers are starting to distribute their ransomware through other means, such as brute-forcing passwords and manual launching. These numbers do not include the many computers around the world unprotected by our solutions that fell victim to WannaCry – this number has been estimated at around 727,000 unique IP addresses.

- WannaCry, ExPetr and BadRabbit notwithstanding, the number of attacks targeting corporates increased only slightly: 26.2% in 2017 compared to 22.6% in 2016. Just over 4% of those targeted in 2017 were SMBs.

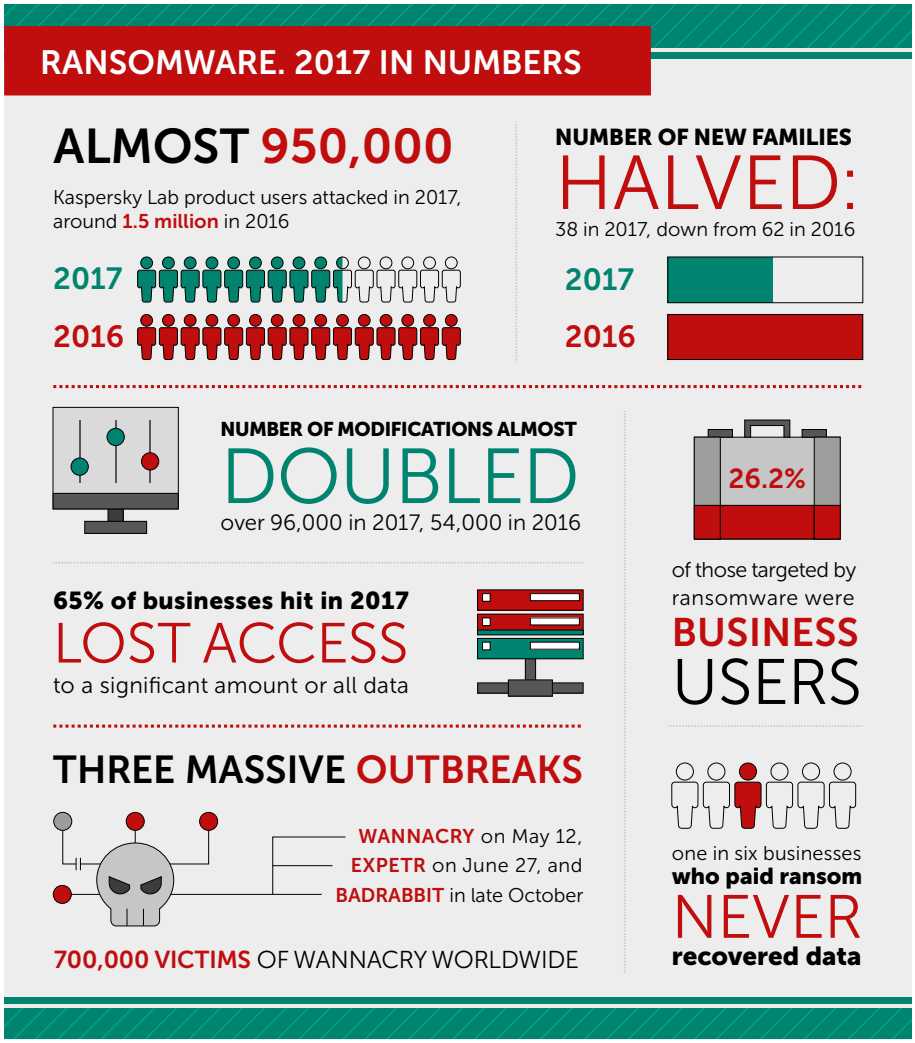
Further details on these trends, including the most affected countries and top ransomware families, can be found in the Kaspersky Security Bulletin 2017 Statistics Report.

According to Kaspersky Lab's annual IT security survey[i]

65% of businesses that were hit by ransomware in 2017 said they lost access to a significant amount or even all their data; while 29% said that although they were able to decrypt their data, a significant number of files were lost forever. These figures are largely consistent with those for 2016.

34% of those affected took a week if not more to restore full access, up from 29% in 2016.

36% paid the ransom – but 17% of them never recovered their data (32 and 19% in 2016).



[i] B2B International IT security survey with Kaspersky Lab, 2017

CONCLUSION: WHAT NEXT FOR RANSOMWARE?

In 2017, we saw ransomware apparently being used by advanced threat actors to mount attacks for data destruction rather than for pure financial gain. The number of attacks on consumers, SMBs and enterprises remained high, but they mainly involved existing or modified code from known or generic families.

Is the ransomware business model starting to crack? Is there a more lucrative alternative for cybercriminals motivated by financial gain? One possibility could be cryptocurrency mining. Kaspersky Lab's threat predictions for cryptocurrencies in 2018 suggest a rise in targeted attacks for the purpose of installing miners. While ransomware provides a potentially large but one-off income, miners can result in lower but longer earnings, and this could be a tempting prospect for many attackers in ransomware's current turbulent landscape. But one thing's for sure, ransomware won't just disappear – neither as a direct threat, nor as a disguise for deeper attacks.

THE FIGHT AGAINST RANSOMWARE CONTINUES

Through collaboration: On July 25, 2016, the No More Ransom initiative was launched by Kaspersky Lab, the Dutch National Police, Europol, and McAfee. It is a unique example of the power of joint public-private collaboration to both fight cybercriminals and help their victims with expertise, tips and decryption tools. One year on, the project has 109 partners and is available in 26 languages. The online portal carries 54 decryption tools, which between them cover 104 families of ransomware. To date, more than 28,000 devices have been decrypted, depriving cybercriminals of an estimated US$9.5 million in ransom.

Through intelligence: Kaspersky Lab has monitored the ransomware threat from the start, and was one of the first to provide regular threat intelligence updates on extortion malware in order to boost industry awareness. The company publishes regular overviews of the evolving ransomware landscape, for instance, here and here.

Through technology: Kaspersky Lab offers multi-layered protection against this widespread and increasing threat, including a free anti-ransomware tool that anyone can download and use, regardless of the security solution they use. The company's products include a further layer of technology: System Watcher that can block and roll back malicious changes made on a device, such as the encryption of files or blocked access to the monitor.

KASPERSKY lab