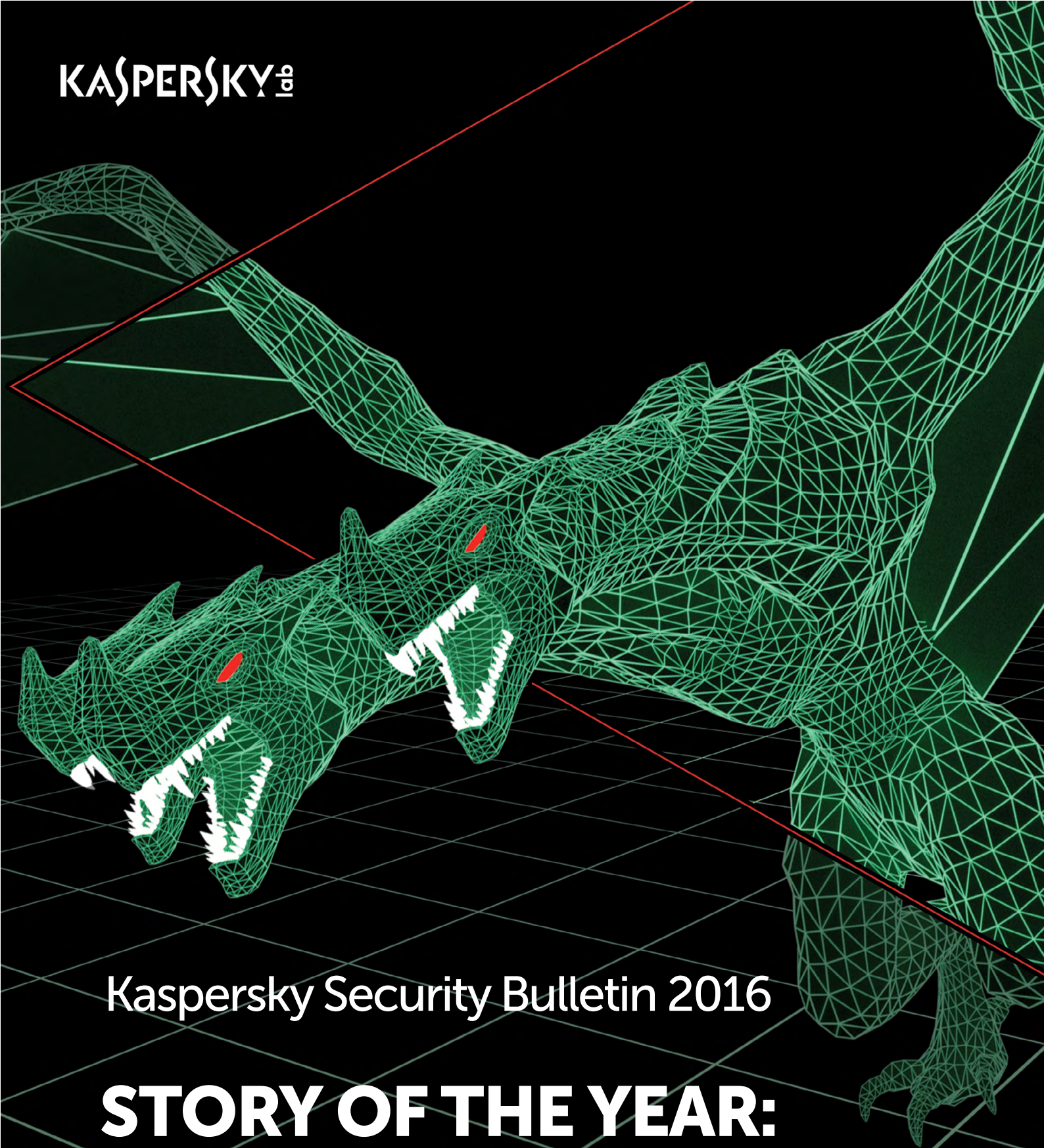
KASPERSKY lab



Kaspersky Security Bulletin 2016

STORY OF THE YEAR: THE RANSOMWARE REVOLUTION

GREAT

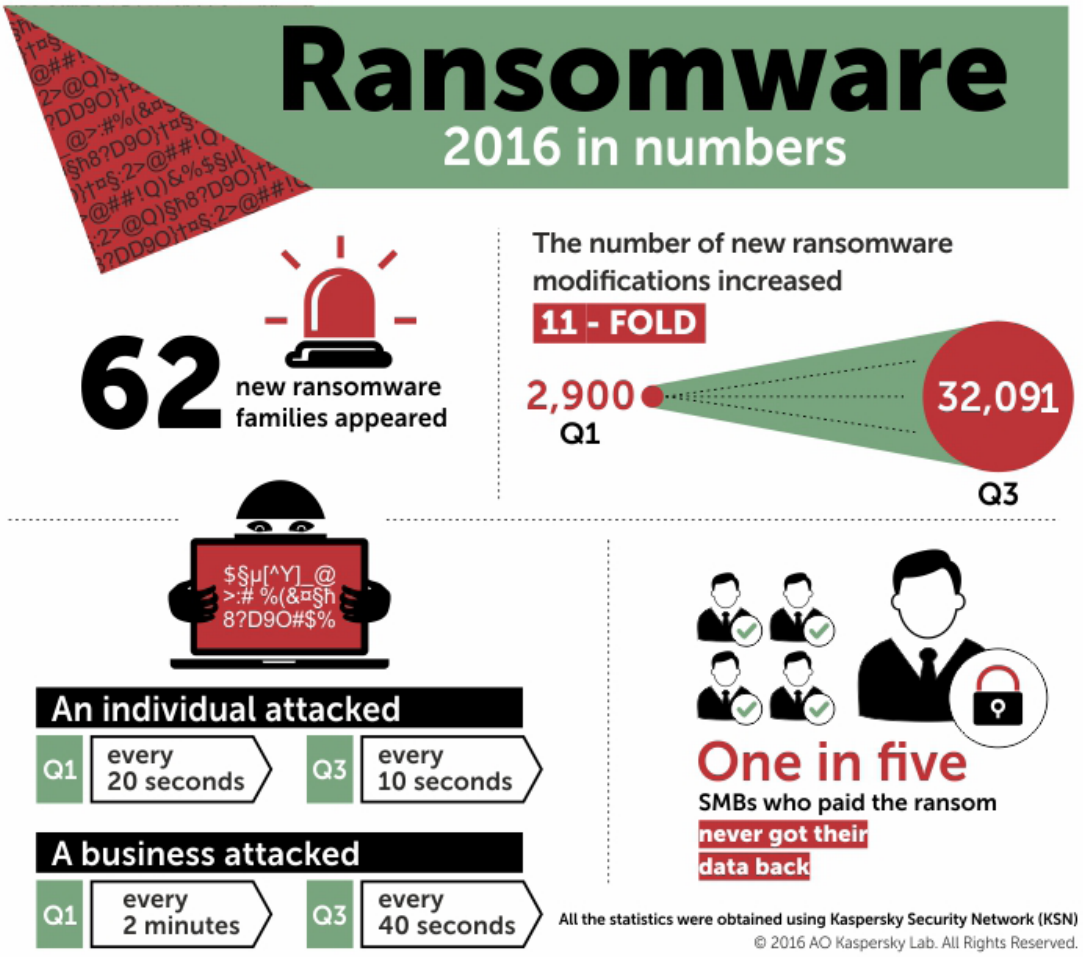
CONTENTS

INTRODUCTION

In 2016, ransomware continued its rampage across the world, tightening its hold on data and devices, and on individuals and businesses.

The numbers speak for themselves:

- 62 new ransomware families made their appearance.
- There was an 11-fold increase in the number of ransomware modifications: from 2,900 new modifications in January/March, to 32,091 in July/September.
- Attacks on business increased three-fold between January and the end of September: the difference between an attack every 2 minutes and one every 40 seconds.
- For individuals the rate of increase went from every 20 seconds to every 10 seconds.
- One in five small and medium-sized business who paid the ransom never got their data back.



2016 also saw ransomware grow in sophistication and diversity, for example: changing tack if it encountered financial software, written in scripting languages, exploiting new infection paths, becoming more targeted, and offering turn-key ransomware-as-a-service solutions to those with fewer skills, resources or time – all through a growing and increasingly efficient underground ecosystem.

At the same time, 2016 saw the world begin to unite to fight back:

The No More Ransom project was launched in July, bringing together the Dutch National Police, Europol, Intel Security and Kaspersky Lab. A further 13 organizations joined in October. Among other things, the collaboration has resulted in a number of free online decryption tools that have so far helped thousands of ransomware victims to recover their data.

This is just the tip of the iceberg – much remains to be done. Together we can achieve far more than any of us can on our own.

What is ransomware?

Ransomware comes in two forms. The most common form of ransomware is the cryptor. These programs encrypt data on the victim's device and demand money in return for a promise to restore the data. Blockers, by contrast, don't affect the data stored on the device. Instead, they prevent the victim from accessing the device. The ransom demand, displayed across the screen, typically masquerades as a notice from a law enforcement agency, reporting that the victim has accessed illegal web content and indicating that they must pay a spot-fine. You can find an overview of both forms of ransomware here.

RANSOMWARE: THE MAIN TRENDS & DISCOVERIES OF 2016

"Most ransomware thrives on an unlikely relationship of trust between the victim and their attacker: that, once payment is received, the ransomed files will be returned. Cybercriminals have exhibited a surprising semblance of professionalism in fulfilling this promise."

GReAT, Threat Predictions for 2017

Arrivals and departures

Arrivals: in 2016, the world said hello to Cerber, Locky and CryptXXX – as well as 44,287 new ransomware modifications

Locky ransomware has so far been spread across

114

countries

Cerber and Locky arrived in the early Spring. Both are nasty, virulent strains of ransomware that are propagated widely, mainly through spam attachments and exploit kits. They rapidly established themselves as 'major players', targeting individuals and corporates. Not far behind them was CryptXXX. All three families continue to evolve and to hold the world to ransom alongside well-established incumbents such as CTB-Locker, CryptoWall and Shade.

As of October 2016, the top ransomware families detected by Kaspersky Lab products look like this:

	Name	Verdicts*	Percentage of users**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25.32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7.07
3	TeslaCrypt (active till May 2016)	Trojan-Ransom.Win32.Bitman	6.54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2.85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2.79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2.36
7	Shade	Trojan-Ransom.Win32.Shade	1.73
8	(generic verdict)	Trojan-Ransom.Win32.Snocry	1.26
9	Crysis	Trojan-Ransom.Win32.Crusis	1.15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0.90

* These statistics are based on the detection verdicts returned by Kaspersky Lab products, received from used of Kaspersky Lab products who have consented to provide their statistical data.

** Percentage of users targeted by a certain crypto-ransomware family relative to all users targeted with crypto-ransomware.

Departures: goodbye to Teslascrypt, Chimera and Wildfire – or so it seemed...

Probably the biggest surprise of 2016 was the shutdown of TeslaCrypt and the subsequent release of the master key, apparently by the malware actors themselves.

TeslaCrypt "committed suicide" – while the police shut down Encryptor RaaS and Wildfire

Encryptor RaaS, one of the first Trojans to offer a Ransomware-as-a-Service model to other criminals shut up shop after part of its botnet was taken down by the police.

Then, in July, approximately 3,500 keys for the Chimera ransomware were publicly released by someone claiming to be behind the Petya/Mischa ransomware. However, since Petya used some of the Chimera source code for its own ransomware, it could in fact be the same group, simply updating its product suite and causing mischief.

Similarly, Wildfire, whose servers were seized and a decryption key developed following a combined effort by Kaspersky Lab, Intel Security and the Dutch Police, now appears to have re-emerged as Hades.

Abuse of 'educational' ransomware

Well-intentioned researchers developed 'educational' ransomware to give system administrators a tool to simulate a ransomware attack and test their defenses. Criminals were quick to seize upon these tools for their own malicious purposes.

Ransomware developed for 'education' gave rise to Ded Cryptor and Fantom, among others

The developer of the educational ransomware Hidden Tear & EDA2 helpfully posted the source code on GitHub. Inevitably, 2016 saw the appearance of numerous malicious Trojans based on this code. This included Ded Cryptor, which changed the wallpaper on a victim computer to a picture of an evil-looking Santa Claus, and demanded a massive two Bitcoins (around $1,300) as a ransom. Another such program was Fantom, which simulated a genuine-looking Windows update screen.

Unconventional approaches

Attackers are now targeting back-ups and hard drives – and brute-forcing passwords

- Why bother with a file when you can have the disk?

  New approaches to ransomware attacks that were seen for the first time in 2016 included disk encryption, where attackers block access to, or encrypt, all the files at once. Petya is an example of this, scrambling the master index of a user's hard drive and making a reboot impossible. Another Trojan, Dcryptor, also known as Mamba, went one step further, locking down the entire hard drive. This ransomware is particularly unpleasant, scrambling every disk sector including the operating system, apps, shared files and all personal data – using a copy of the open source DiskCryptor software.

- The 'manual' infection technique

  Dcrypter's infection is carried out manually, with the attackers brute-forcing passwords for remote access to a victim machine. Although not new, this approach has become significantly more prominent in 2016, often as a way to target servers and gain entry into a corporate system.

  If the attack succeeds, the Trojan installs and encrypts the files on the server and possibly even on all the network shares accessible from it. We discovered TeamXRat taking this approach to spread its ransomware on Brazilian servers.

Shade downloaded spyware if it found financial software

- Two-in-one infection

  In August we discovered a sample of Shade that had unexpected functionality: if an infected computer turned out to belong to financial services, it would instead download and install a piece of spyware, possibly with the longer term aim of stealing money.

Ransomware in scripting languages

Another trend that attracted our attention in 2016 was the growing number of cryptors written in scripting languages. In the third quarter alone, we came across several new families written in Python, including HolyCrypt and CryPy, as well as Stampado written in AutoIt, the automation language.

A long line of amateurs and copycats

Poor quality ransomware increases likelihood of data being lost forever

Many of the new ransomware Trojans detected in 2016 turned out to be of low-quality; unsophisticated, with software flaws and sloppy errors in the ransom notes.

This was accompanied by a rise in copycat ransomware. Among other things, we spotted that:

- Bart copies the ransom note & the style of Locky's payment page.
- An Autoit-based copycat of Locky (dubbed AutoLocky) uses the same extension ".locky".
- Crusis (aka Crysis) copies the extension ".xtbl" originally used by Shade.
- Xorist copies the whole naming scheme of the files encrypted by Crusis.

Probably the most prominent copycat we discovered this year was Polyglot (aka MarsJoke). It fully mimics the appearance and file processing approach of CTB-Locker.

These trends are all expected to increase in 2017.

"As the popularity continues to rise and a lesser grade of criminal decides to enter the space, we are likely to encounter more and more 'ransomware' that lacks the quality assurance or general coding capability to actually uphold this promise. We expect 'skiddie' ransomware to lock away files or system access or simply delete the files, trick the victim into paying the ransom, and provide nothing in return."

GReAT, Threat Predictions for 2017

THE THRIVING RANSOMWARE ECONOMY

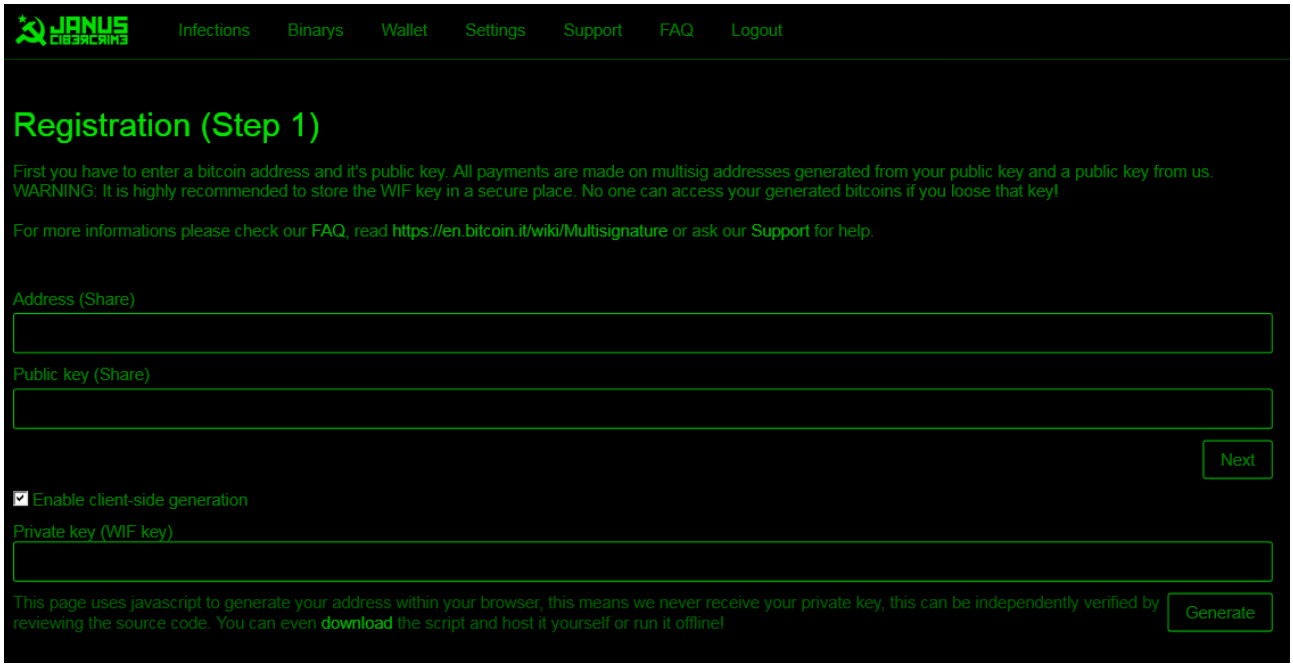
The rise of RaaS

Ransomware is increasingly for hire on the criminal underground

While Ransomware-as-a-Service is not a new trend, in 2016 this propagation model continued to develop, with ever more ransomware creators offering their malicious product 'on demand'. This approach has proved immensely appealing to criminals who lack the skills, resources or inclination to develop their own.

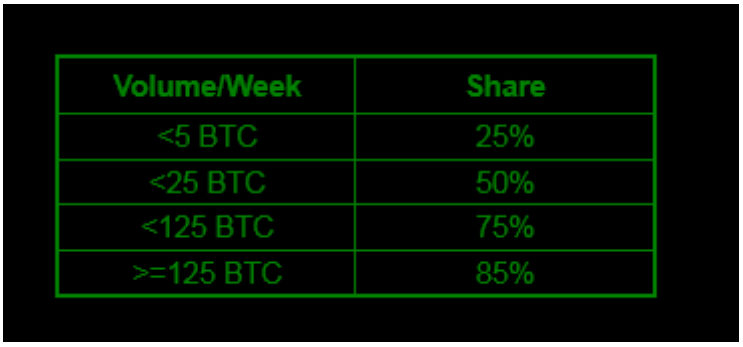
Notable examples of ransomware that appeared in 2016 and use this model are Petya/Mischa and Shark ransomware, which was later rebranded under the name Atom.

This business model is increasingly sophisticated:



The Petya ransomware partner site

The partner often signs up to a traditional commission-based arrangement. For example, the 'payment table' for Petya ransomware shows that if a partner makes 125 Bitcoins a week thy will walk away with 106.25 Bitcoins after commission.



Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Petya payment table

There is also an initial usage fee. Someone looking to use the Stompado ransomware, for example, needs to come up with just $39.

With other criminals offering their services in spam distribution, ransomware notes etc. it's not difficult for an aspiring attacker to get started.

From commission-based networks to customer support and branding

Criminals offer customer support to ensure more victims pay

The most 'professional' attackers offered their victims a help desk and technical support, guiding them through the process of buying Bitcoins to pay the ransom, and sometimes even being open to negotiation. Every step further encouraged the victim to pay.

Further, Kaspersky Lab experts studying ransomware in Brazil noticed that for many attacks, branding the ransomware was a matter of some importance. Those looking for media attention and customer fear would opt for a high profile, celebrity theme or gimmick – while those more concerned about staying under the radar would forgo the temptation of fame and leave their victims facing just an e-mail for contacting the bad guys and a Bitcoin address to pay into.

It's still all about the Bitcoins

Throughout 2016, the most popular ransomware families still favored payment in Bitcoins. Most ransomware demands were not excessive, averaging at around $300, although some were charged – and paid – a great deal more.

Others, particularly regional and hand-crafted operations, often preferred a local payment option – although this also meant that they were no longer able to hide in plain sight and blend in with the rest of the ransomware noise.

RANSOMWARE TURNED ITS WEAPONS ON BUSINESS

A business is attacked with ransomware every 40 seconds

In the first three months of 2016, 17% of ransomware attacks targeted corporates – this equates to an attack hitting a business somewhere in the world every two minutes*. By the end of Q3 this had increased to 23.9% – an attack every 40 seconds.

According to Kaspersky Lab research, in 2016, one in every five businesses worldwide suffered an IT security incident as a result of a ransomware attack.

- 42% of small and medium-sized businesses were hit by ransomware in the last 12 months.
- 32% of them paid the ransom.
- One in five never got their files back, even after paying.
- 67% of those affected by ransomware lost part or all of their corporate data – and one- in-four spent several weeks trying to restore access.

* Estimates based on: 17% of 372,602 unique users with ransomware attacks blocked by Kaspersky Lab products in Q1, 2016 and 23.9% of 821,865 unique users with ransomware attacks blocked by Kaspersky Lab products in Q3,2016.

One in five SMBs never gets their data back, even after paying

There is no such thing as a low-risk sector anymore

Social engineering and human error remain key factors in corporate vulnerability. One in five cases involving significant data loss came about through employee carelessness or lack of awareness.

Some industry sectors are harder hit than others, but our research shows that all are at risk.

	Industry sector	% attacked with ransomware
1	Education	23
2	IT/Telecoms	22
3	Entertainment/Media	21
4	Financial Services	21
5	Construction	19
6	Government/public sector/defence	18
7	Manufacturing	18
8	Transport	17
9	Healthcare	16
10	Retail/wholesale/leisure	16

"We are seeing more targeted ransomware, where criminal groups carefully hand-pick and spear-phish their targets because of the data they possess and/or their reliance on the availability of this valuable data."

John Fokker, Digital team Coordinator
with the Dutch National High Tech Crime unit

Ransomware attacks that made the headlines

- **Hospitals became a prime target** – with potentially devastating impact as operations were cancelled, patients diverted to other hospitals and more.
  - The most notorious example of a ransomware attack took place in March when criminals locked down the computers of the Hollywood Presbyterian Medical Center in Los Angeles, until the hospital paid $17,000.
  - Within weeks, a number of hospitals in Germany were also hit.
  - In the UK, 28 National Health Service trusts admit to being attacked in 2016.
- **Hosted desktop and cloud provider** VESK paid nearly $23,000 dollars in ransom to recover access to one of its systems following an attack in September.
- **Leading media**, including the New York Times, the BBC and AOL were hit by malware carrying ransomware in March 2016.
- **The University of Calgary in Canada**, a major research center, acknowledged it had paid around $16,000 to recover emails that been encrypted for a week.
- A **small police station** in Massachusetts, ended paying a $500 ransom (via Bitcoin) in order to retrieve essential case-related data, after an officer opened a poisonous email attachment.
- **Even motor racing was hit:** a leading NASCAR racing team faced losing data worth millions to a TeslaCrypt attack in April.

FIGHTING BACK

Through technology

The latest versions of Kaspersky Lab products for smaller companies have been enhanced with anti-cryptomalware functionality. In addition, a new, free anti-ransomware tool has been made available for all businesses to download and use, regardless of the security solution they use.

A new free, AV-independent anti-ransomware tool is available

Kaspersky Lab's Anti-Ransomware Tool for Business is a 'light' solution that can function in parallel with other antivirus software. The tool uses two components needed for the early detection of Trojans: the distributed Kaspersky Security Network and System Watcher, which monitors applications' activity.

Kaspersky Security Network quickly checks the reputation of files and website URLs through the cloud, and System Watcher monitors the behavior of programs, and provides proactive protection from yet-unknown versions of Trojans. Most importantly, the tool can back up files opened by suspicious applications and roll back the changes if the actions taken by programs prove malicious.

Through collaboration: The No More Ransom Initiative

No More Ransom has so far got 4,400 people their data back – and deprived criminals of $1.5 million in ransom

On 25 July 2016, the Dutch National Police, Europol, Intel Security and Kaspersky Lab announced the launch of the No More Ransom project – a non-commercial initiative that unites public and private organizations and aims to inform people of the dangers of ransomware and help them to recover their data.

The online portal currently carries eight decryption tools, five of which were made by Kaspersky Lab. These can help to restore files encrypted by more than 20 types of cryptomalware. To date, more than 4,400 victims have got their data back – and more than $1.5 million dollars in ransom demands has been saved.

In October, law enforcement agencies from a further 13 countries joined the project, including: Bosnia and Herzegovina, Bulgaria, Colombia, France, Hungary, Ireland, Italy, Latvia, Lithuania, Portugal, Spain, Switzerland and the United Kingdom.

Eurojust and the European Commission also support the project's objectives, and more partners from the private sector and law enforcement are expected to be announced soon.

"Public/Private partnerships are the essence and the strength of the NMR initiative. They are essential to effectively and efficiently tackle the problem, providing us with much greater capability and reach than law enforcement could have alone."

Steven Wilson, Head of Europol's EC3

Standing up to ransomware – how to stay safe

1. Back up data regularly.
2. Use a reliable security solution, and remember to keep key features – such as System Watcher – switched on.
3. Always keep software updated on all the devices you use.
4. Treat email attachments, or messages from people you don't know, with caution. If in doubt, don't open it.
5. If you're a business, you should also educate your employees and IT teams; keep sensitive data separate; restrict access; and back up everything, always.
6. If you are unlucky enough to fall victim to an encryptor, don't panic. Use a clean system to check our No More Ransom site; you may well find a decryption tool that can help you get your files back.
7. Last, but not least, remember that ransomware is a criminal offence. Report it to your local law enforcement agency.

Why you shouldn't pay – advice from the Dutch National High Tech Crime Unit

1. You become a bigger target.
2. You can't trust criminals – you may never get your data back, even if you pay.
3. Your next ransom will be higher.
4. You encourage the criminals.

"We urge people to report an attack. Every victim holds an essential piece of evidence that provides invaluable insight. In return, we can keep them informed and protect them from dodgy third-party 'offers' to unencrypt data. But we need to ensure that more law enforcement offices know how to deal with digital crime."

Ton Maas, Digital team Coordinator
with the Dutch National High Tech Crime unit

CAN WE EVER WIN THE FIGHT AGAINST RANSOMWARE?

We believe we can – but only by working together. Ransomware is a lucrative criminal business. To make it stop the world needs to unite to disrupt the criminals' kill-chain and make it increasingly difficult for them to implement and profit from their attacks.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy