Paper

Bitdefender

Ransomware targets SMBs due to weaker protection and greater willingness to pay up

Attackers are now targeting small and medium businesses to extort higher fees, a Bitdefender survey shows, meeting the company's predictions for 2017.

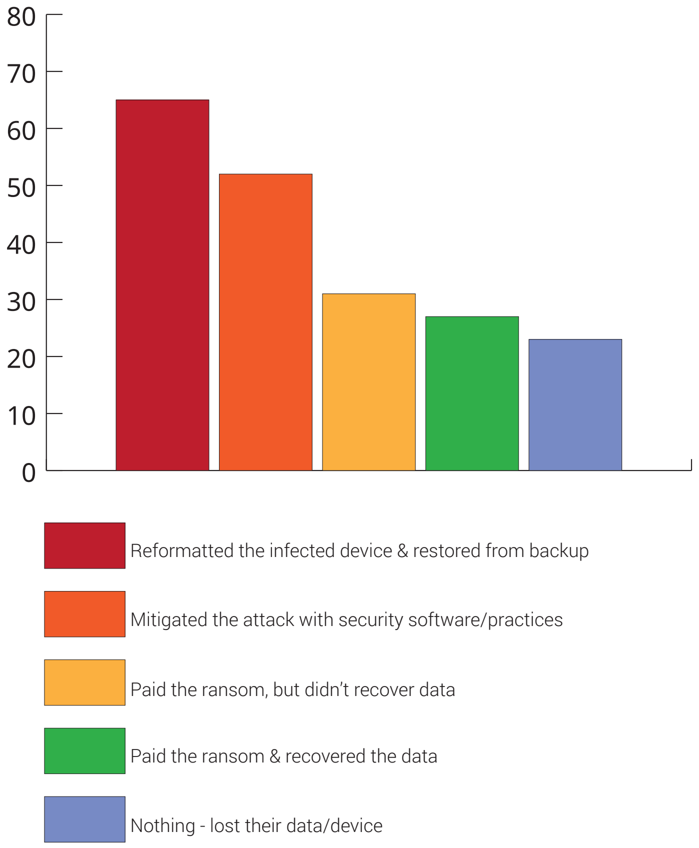
One in five small and medium businesses (SMBs) in the US reported a ransomware attack within the past 12 months, according to a Bitdefender survey of 250 IT pros in the US working in SMBs, carried out by Spiceworks. Some 38% indicated they paid ransom - $2,423 on average - but most did not recover the encrypted data.

Ransomware, a type of malware that locks and usually encrypts a computer's files until the victim pays to regain access, is the fastest-growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016, a 300-percent increase over the approximately 1,000 attacks per day seen in 2015, according to the U.S. Department of Justice. SMBs are ideal targets for ransomware developers as some do not invest in security solutions, yet they handle sensitive business information (i.e. customer data, financial records, product info), targets that cyber-criminals value most.

Bitdefender's survey shows that less than half (45%) of the SMBs that paid to regain access to their data after falling victim to ransomware actually got their information back.

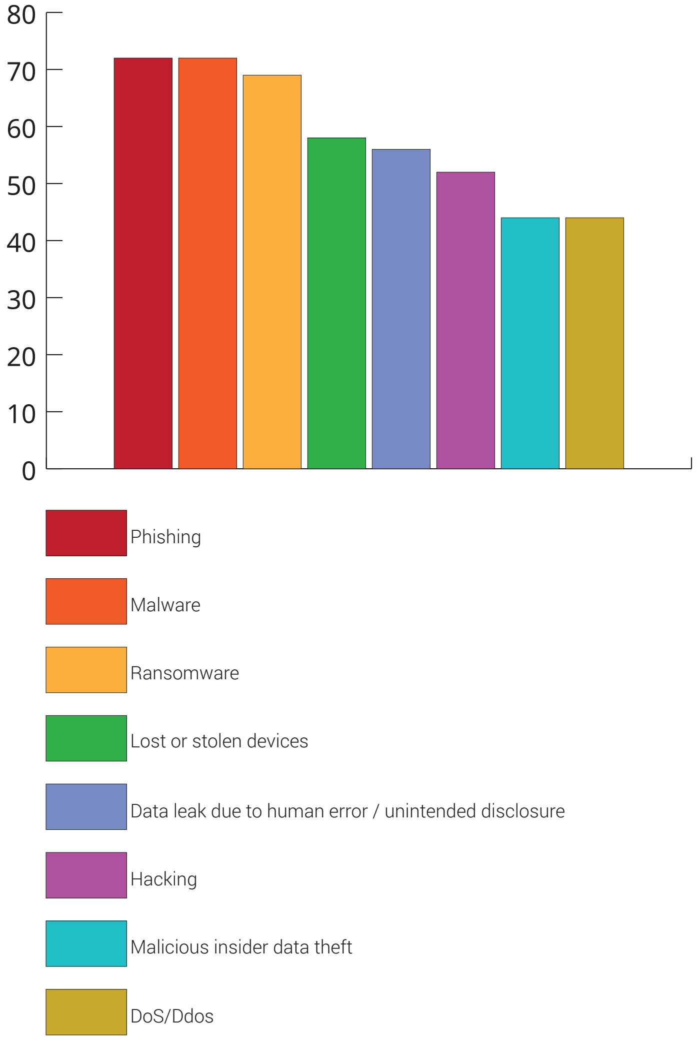
From those targeted, most were able to mitigate the attack by restoring from backup (65%) or through security software/practices (52%). A quarter of those targeted couldn't find a solution to address the ransomware attack and lost their data.

How SMBs addressed the ransomware attack (%)



Though relatively few organizations have recent experience with ransomware attacks, the threat is alarming. Some 69% of the participating IT pros expressed concern about ransomware, on par with their concerns about phishing (72%), and malware (72%). Nearly half of US SMBs also fear incidents stemming from lost or stolen devices, unintended disclosure / data leak due to human error, hacking, malicious insider data theft, or DoS/DDoS attacks.

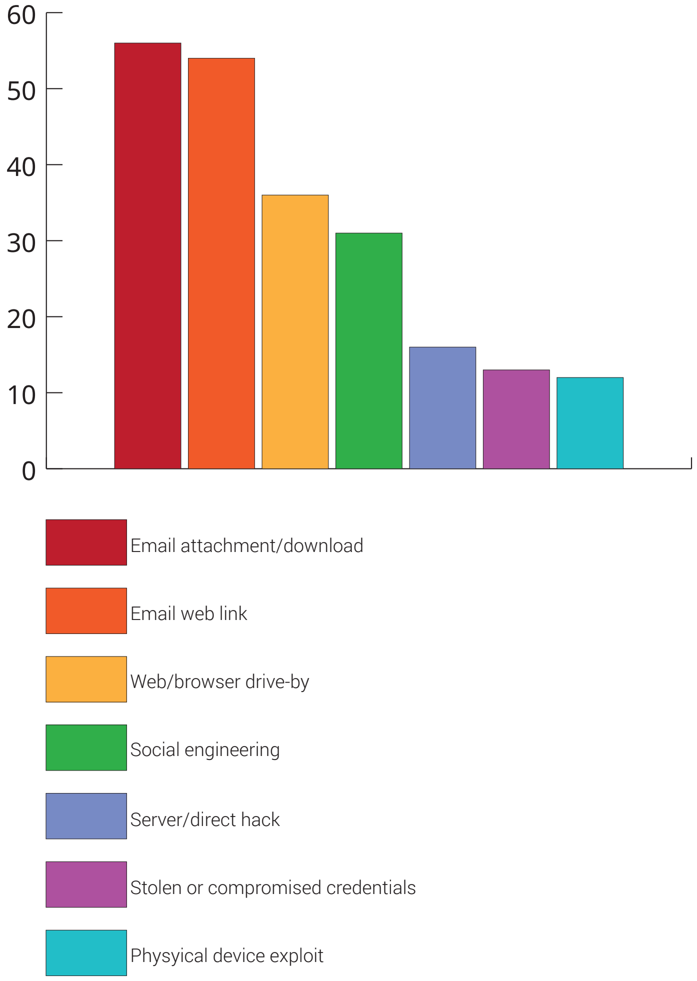
Concerns about experiencing the following IT security threat in the next year (%)



For those who experienced a breach in the past 12 months, the main vector of attack was e-mail (77%). Through email, attackers were able to provoke a user via attachment/download (56%) or web link (54%). 36% were web/browser drive-by, and 31% occurred through social engineering.

The outcomes of this survey support Bitdefender's predictions in the cyber threat landscape for 2017, particularly that ransomware will become more prevalent than ever.

Attack vector of the IT security threat/breach (%)



“Building on the massive financial milestones in 2016, ransomware operations will likely dedicate more resources to improving automated targeting in 2017,” Bitdefender security specialists predicted. This feature will help them discriminate between home users and corporations so they can focus on extorting higher ransoms from the latter. Holding SMBs to ransom can increase cyber criminals’ return on investment five-fold, as half of individuals are willing to pay up to $400-500 to recover their data, while SMBs would pay $2,500 on average. Initially, consumer victims have brought the ransomware business staggering amounts of money, but attackers now aim to increase their gains without increasing their effort, and further fuel the ransomware-as-a-service business model.

2016 was arguably the year of ransomware, and this threat will continue to proliferate in 2017, sparing no operating system or platform – Windows, Android, Linux, and Mac OS. Data extracted from Bitdefender’s telemetry, as well as intelligence collected from exposed command and control servers and compromised botnets, suggests that ransomware operation is a crime that still pays - and very well indeed. One particular ransomware botnet Bitdefender was monitoring raked in $1.5 million in just one week of operation last year.

However, paying ransom does not guarantee an organization will regain access to its data. Some individuals or organizations were never given decryption keys after paying ransom. What’s more, some victims who paid were targeted again. After paying the originally demanded ransom, some victims were asked to pay more for the promised decryption key. It’s also worth mentioning that paying could encourage this criminal business model, the U.S. government says.

The survey also shows that the most common IT security solutions used by US SMBs to protect themselves against ransomware and other online threats include anti-malware and endpoint security (80%), network firewalls (72%), email security solutions (71%) and client firewalls (71%).

SMBs can also be perceived by attackers as a small piece of a bigger puzzle. If they do business with larger companies, most likely they are being used to get to the ultimate target. Unfortunately, due to a lack of dedicated budgets for security, entrepreneurs put security on the back burner of their business priorities. Moreover, they underestimate the impact a proprietary information leak may have on their reputation, credibility and, ultimately, profits.

As their budget is likely to be tight, SMBs should invest in products that address particular needs or weaknesses, such as blocking sophisticated malware or ensuring employees have secure and authorized access to networks and data, Bitdefender's security specialists recommend.

On behalf of Bitdefender, Spiceworks surveyed, in February 2017, 250 IT pros in the US working in SMBs.

To stay safe from ransomware, SMBs are strongly encouraged to:

- Use an endpoint security solution

- Patch or update all endpoint software and webservers

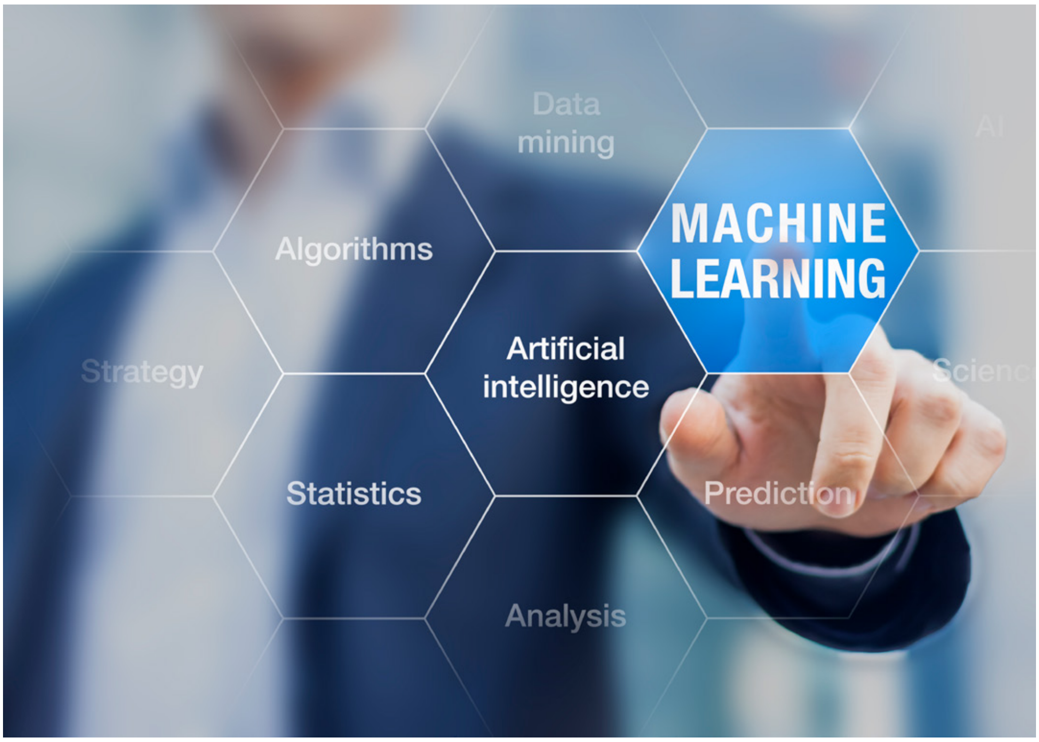
- Deploy a backup solution

- Disable files from running in locations such as "AppData/LocalAppData" and deploy policies that restrict users from executing malware

- Limit users from accessing mapped network drives

- Protect email servers with content filtering solutions

- Educate employees on identifying spear-phishing emails and other social engineering techniques.



Patented Machine Learning in Ransomware Detection

With more than 7 issued patents for using machine learning algorithms in detecting malware and other online threats, the use of deep learning and anomaly-based detection techniques play a vital role in proactively fighting new and unknown threats. Ransomware has not only become a scourge for Windows-based operating systems, but it has also targeted Android mobile operating system for years. With financial losses estimated in the hundreds of millions, some estimating that it's could reach close to one billion dollars by the end of 2016, traditional security mechanism and technologies have fell short of completely protecting against it.

At Bitdefender we've been working on machine learning algorithms since 2009, constantly developing and training them to identify new and unknown threats. Artificial Intelligence and machine learning are essential to combat a threat landscape that is larger and more sophisticated than ever. Bitdefender has more than eight years of experience in perfecting these technologies and the results clearly show this: better detection rates with fewer false positives.

Machine learning algorithms have the ability to significantly improve detection time for ransomware threats, as they're able to analyze large amounts of data significantly faster than any human would. If properly trained to accurately detect various types of ransomware behavior, machine learning algorithms can have a high detection rate even on new or unknown samples. The merging of human ingenuity with machine learning speed and relentless data analysis, significantly reduces reaction time against new ransomware samples, offering protection even from previously unknown ransomware samples. However, it's not always just a single machine learning algorithm doing the detection.

Detecting ransomware requires the use of several algorithms, each specialized in detecting specific ransomware families with individual behaviors. This significantly increases the chances of detecting similarly-looking ransomware while reduces the amount of false positives. By training machine learning algorithms on large datasets of ransomware samples, they're able to quickly reveal indicators of compromise and help the security solution prevent new or unknown ransomware samples from encrypting files.

Multiple anti-ransomware defenses with Bitdefender Gravity Zone

Using advanced behavior-based technologies, Bitdefender detected 99% of unknown threats in independent trials run by reputed independent testing organization, AV-Comparatives. Bitdefender Advanced Threat Control (ATC) permanently monitors running processes for signs of malicious behavior. A pioneering technology launched in 2008 as AVC (Active Virus Control), ATC has constantly been enhanced, keeping Bitdefender one step ahead of emerging threats. Bitdefender also has two additional anti-ransomware defense layers – a blacklist of 2.8 million samples and rising, and a vaccine that can immunize devices against the encryption process.

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/