How patented machine-learning boosts ransomware detection and prevents businesses from being encrypted

By Razvan Muresan on Jan 12, 2017

Ransomware, the most prolific cyber threat of the moment, gains foothold in organizations and companies via file-sharing networks, e-mail attachments, malicious links or compromised websites that allow direct downloads.

According to a Bitdefender study carried in the United States, ransomware is mentioned second in the top CIO concerns for medium and large companies. According to the findings of that study, 13.7 percent of the interviewed companies perceive ransomware as a hard-to-tackle threat. The study also shows that ransomware and rootkits are perceived as particularly difficult to tackle by companies with limited experience in malware attacks. The first quarter of 2016 saw 3,500% growth in the number of ransomware domains created, setting a new record.

Ransomware was seen as a major threat in the top predictions list in cyber security for 2016 by Bitdefender CTO Bogdan Dumitru. In March, Palo Alto Networks researchers revealed KeRanger ransomware targeted Mac users for the first time, realizing Bitdefender's predictions about ransomware's expansion to new operating systems in 2016.

"We've already seen ransomware for Linux, Windows and Android. Mac OS is just around the corner," he said in December 2015. "It targets both consumers and companies, and the 2016 versions not only will encrypt files and ask for ransom, but will also make all documents available on the internet if ransom is not paid. In an ironic twist, the victim will be able to recover encrypted files – when they are uploaded on the internet for public shaming."

"Ransomware has probably been the largest unresolvable threat to Internet users ever since 2014, and it will remain one of the most important drivers of cybercrime in 2016," Bitdefender noted. "While some operators will prefer the file encryption approach, some more innovative groups will focus on developing 'extortionware' (malware that blocks accounts on various online services or that expose data stored locally to everybody on the Internet). Throughout 2016, file-encrypting ransomware will most likely expand to Mac OS X as well."

Recent reports show millions of users fell victim to CryptoWall version 3.0 (and many go unreported), adding over $350 million to cybercriminals' bank accounts.

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. Unlike other vendors, Bitdefender has 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.

Read the full white paper here.

Building on the massive financial milestones aforementioned, ransomware operations will likely dedicate more resources to improving automated targeting in 2017, as Bitdefender experts predict. This feature will help them discriminate between home users and corporations, and trying to extort higher fees from the latter.

2016 was arguably the year of ransomware, and this threat will continue to proliferate in the year to come, sparing no operating system or platform. Data extracted from our

telemetry, as well as intelligence collected from exposed command and control servers and compromised botnets, suggests that ransomware operation is a crime which still pays - and very well indeed.

"One particular ransomware botnet we were monitoring raked in 1.5 million in just one week of operation, earlier this year" explained Bitdefender Chief Security Strategist Catalin Cosoi.

The profitability of such schemes lays in part in the fact that people really do value their private data, although there do seem to be cultural differences even in this field. When surveyed by Bitdefender, only one third (33%) of consumers in Germany have claimed they would pay to regain access to their data if it were held to ransom, while the figure is 50% for the US.