Paper

Bitdefender®

Evolution of Top 3 Threats Reveals that Hype, Maturity and Stealth Drive Cybercrime

Cybercrime is among the fastest-growing crimes globally, with experts estimating financial losses will reach $6 trillion annually by 2021, from $3 trillion in 2015. Threats ranging from zero-days to ransomware and denial of service attacks are predicted to continuously inflict serious damage to organizations and users around the world, but emerging and hyped threats - such as coin mining – are equally as dangerous.

Recent Bitdefender telemetry shows that some of the most popular threats revolve around ransomware, coin miners, and fileless threats. Their adoption and prevalence are based on hype, maturity, and the potential for generating significant revenue in the shortest amount of time. The use of coin miners is a perfect example of threat actors leveraging the hype around cryptocurrency to build cryptocurrency mining operations estimated to net as much as $3 million per campaign.

Abstract

Ransomware has undoubtedly been among the most prevalent threats for the past couple of years, inflicting financial losses estimated in the billions of dollars globally. Its success in generating revenue has even spurred creation of an entire industry – ransomware-as-a-service – where cybercriminals focus on developing tools, offering support, and even implementing business models ranging from upfront payments to subscriptions for anyone interested in starting their own ransomware campaign.

The stability, maturity, and constant development of ransomware has made it a weapon of choice for cybercriminals. While only 50 percent of victims pay ransom, other threats guarantee instant return-on-investment. **Cryptojacking** – or the use of coin mining software to illicitly use a victim's computing power to mine for crypto currency – has become the latest hype.

Although cryptojacking was not even considered a threat at the end of 2017, during the first couple of months of 2018 it was seriously abused by threat actors to generate substantial revenue by placing the mining agent either within compromised high-traffic websites or within organizations with a large pool of computing resources. From September 2017 to January 2018, the number of crypto miner reports has increased by a staggering 130.10 percent, showing that a seemingly benign process can be abused by threat actors.

While both ransomware and coin miners are currently both popular threats for generating revenue, the techniques used by threat actors to disseminate them have grown in sophistication. Because organizations are the ones that cybercriminals usually target to maximize financial output, threat actors have begun abusing **fileless** malware to deploy either ransomware or coin miners within infrastructures.

The use of scripts (such as Visual Basic, PowerShell, etc.) embedded within documents or planted on tampered websites has mainly been associated with advanced threats meant to deliver cyberespionage tools. However, because fileless threats are highly versatile and dodge the security mechanisms of traditional security solutions, they're now being used to deploy ransomware and even coin miners, especially when targeting organizations.

Threat Evolution - UK vs Global Trends

Cyber threats don't usually discriminate based on geographical location, affecting all countries and all users equally. The evolution of ransomware and coin miners has pretty much followed this trend, showing that both locally - for the UK – and globally, threat distribution follows the same trend. In a previous Bitdefender report, ransomware and coin miner distribution in the UK followed the same pattern, showing that when ransomware reports went down, coin miners picked up steam.

The hype around coin miners that started in late 2017 has caused the number of coin miner **reports in the United Kingdom to spike in January 2018 to 22.06 percent** (of the total number of coin mining reports between November 2017 and April 2018).

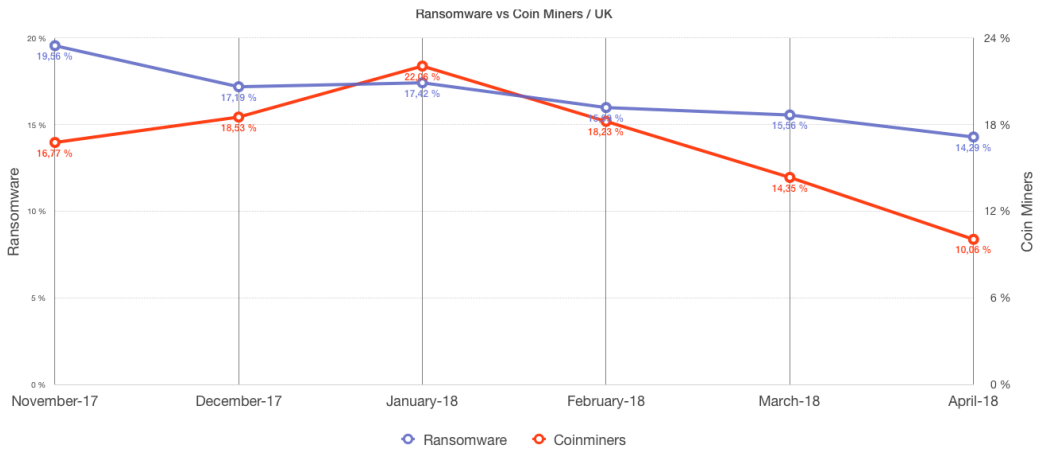

Fig. 1 – Ransomware vs. Coin miners UK evolution

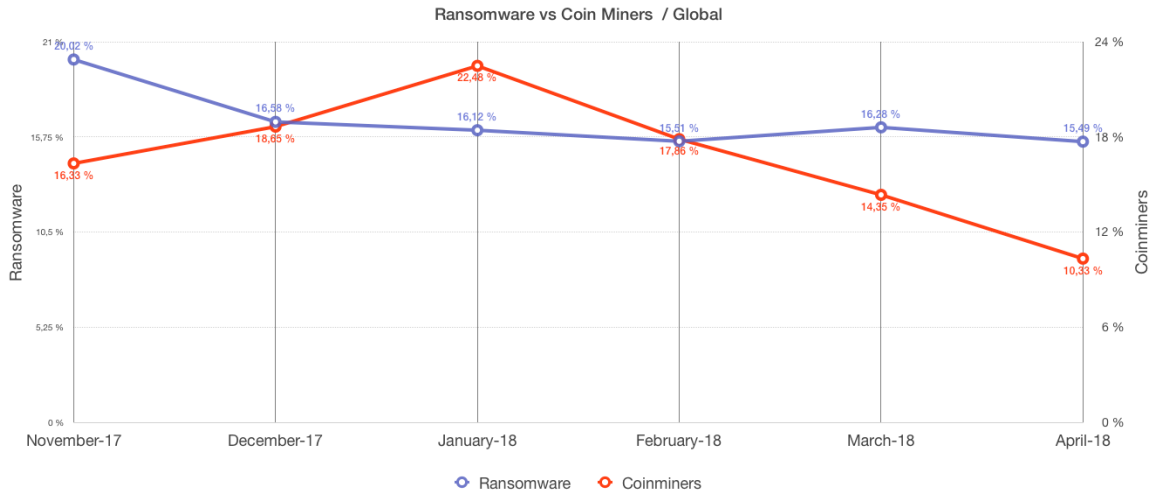

Fig. 2 – Ransomware vs. Coin miners global evolution

The same spike has also been seen on the global scale, as coin miner reports peaked at **22.48 percent** of the total amount of coin miners reported between November 2017 and April 2018. The descending line in cryptojacking reports observed locally for the UK follows the same pattern on the global scale, potentially indicating that threat actors are beginning to lack focus when it comes to choosing a specific crypto currency to mine.

With over 1,500 cryptocurrencies currently available over the internet – specifically, 1565 as of April 10 2018 – threat actors may find it difficult to pick a stable and financially profitable one to mine. If Bitcoin was the preferred currency in late 2017 and early 2017, the below Fig. 3 clearly illustrates a sharp depreciation in its value.

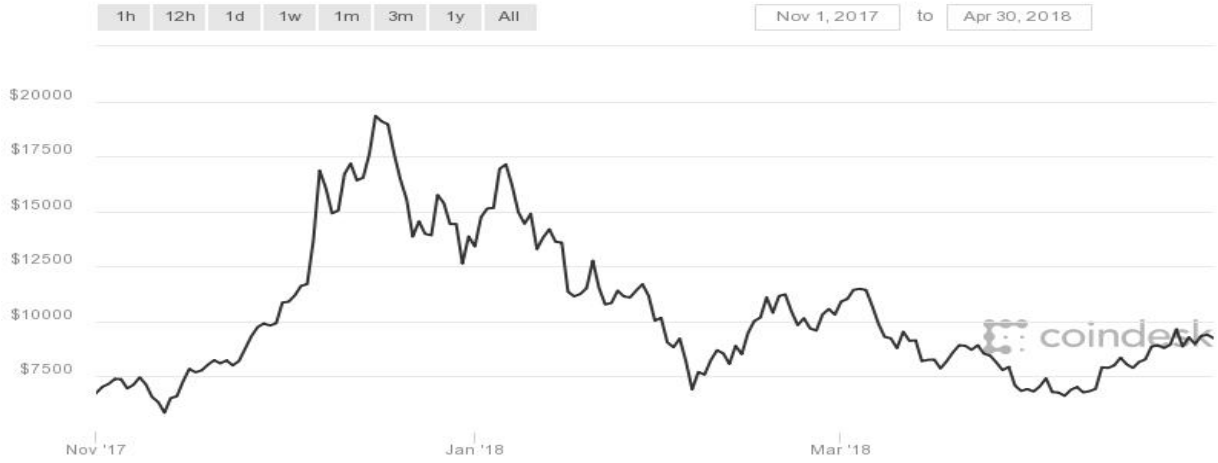

Fig. 3 – Bitcoin price evolution. Source: Coindesk

Alternative currencies, such as Monero and Etherium, have shown some stability over time, but the wide array of available currencies and their volatility may have left threat actors confused as to which one is more profitable in the long run. Even the return on investment is immediate – as a victim will immediately start mining for currency once it's compromised – ransomware does have the benefit of a fixed income, provided the victim gives in.

Because ransomware evolution in the UK has followed a steady pace, only dropping **5.27 percentage** points between November 2017 and April 2018, it's likely threat actors will not give it up easily and we'll see more of it in the next couple of years.

Comparing ransomware reports with the number of reports that involve fileless threats in the UK (January through April 2018), a pattern emerges. While ransomware reports drop from January's **17.42 percent** to **14.29 percent** (of all ransomware reports from January through April), fileless threats drop by **19.04 percent** within the same time.

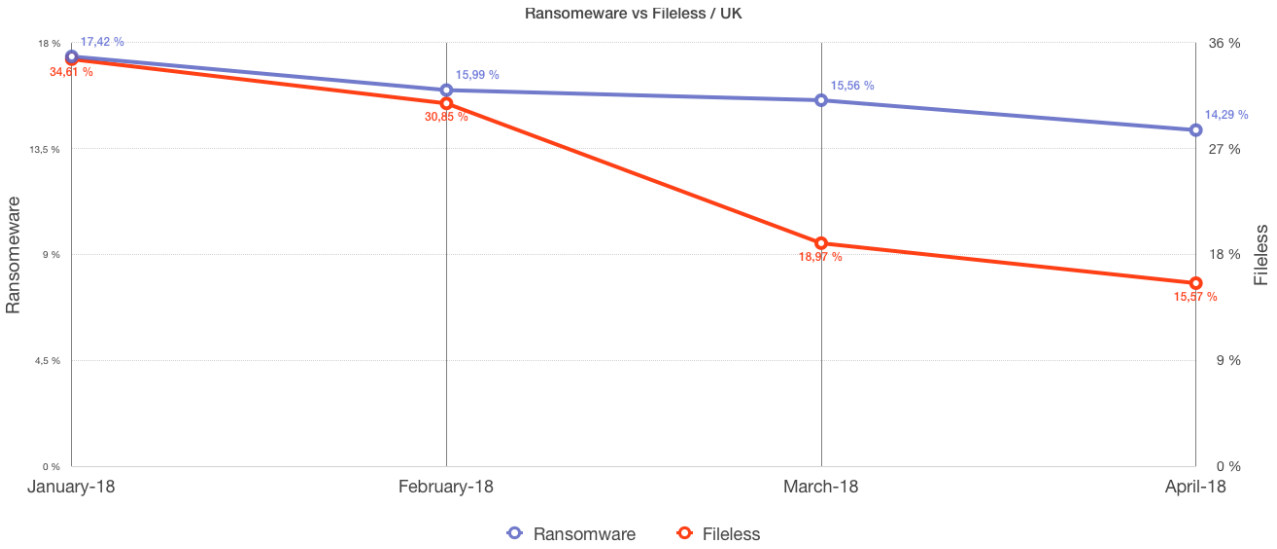

Fig. 4 – Ransomware vs. Fileless UK evolution

While ransomware's maturity explains the relatively low variance in reports across the last four months, the drop in fileless reports in the United Kingdom may have an explanation. It may be more lucrative to deploy ransomware and other threats using traditional mechanisms such as infected websites or email attachments, instead of making use of sophisticated fileless malware.

Globally, both ransomware and fileless reports have followed a descending curve in terms of reports. As previously mentioned, ransomware's maturity explains its steady variance, fileless reports are following the same drop as coin miners (Fig. 5).

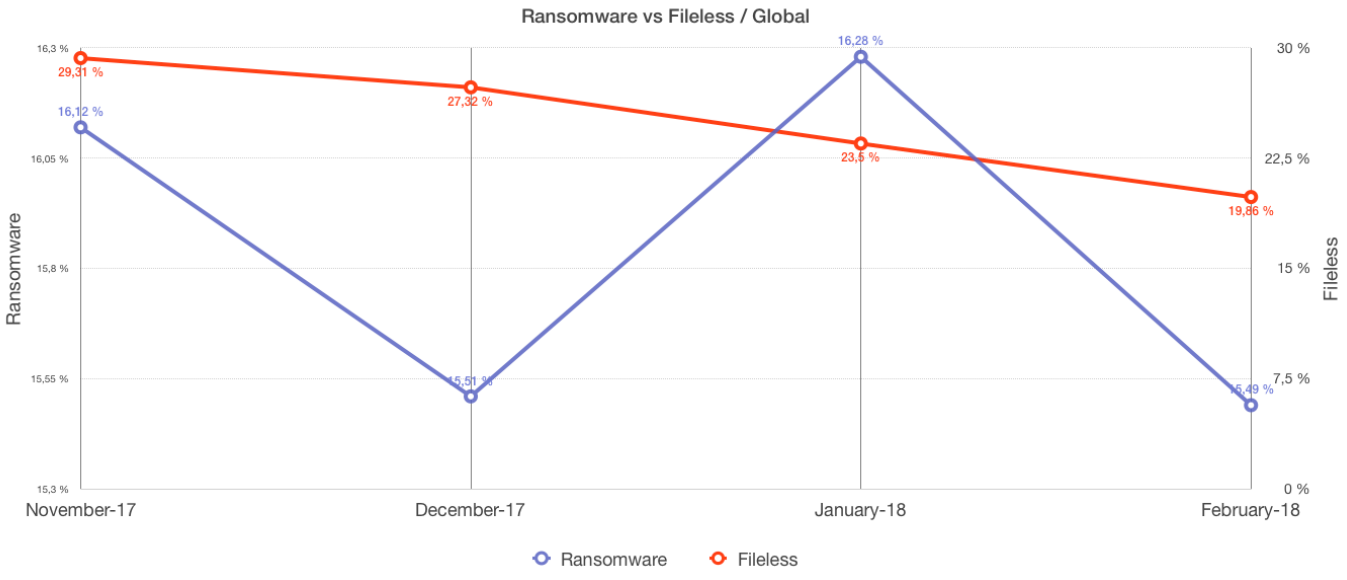

Fig. 5 – Ransomware vs. Fileless global evolution

Interestingly, analysis shows coin miner and fileless reports seem to directly influence each other. As threat actors have in recent months relied on fileless techniques to drop coin miners into organizations' infrastructures, the drop in coin miner reports might have dragged the drop in fileless reports as well. Since they both peaked at the same time and both followed the same descending curve, it's safe to estimate that threat actors have been using fileless techniques to drop coin mining software.

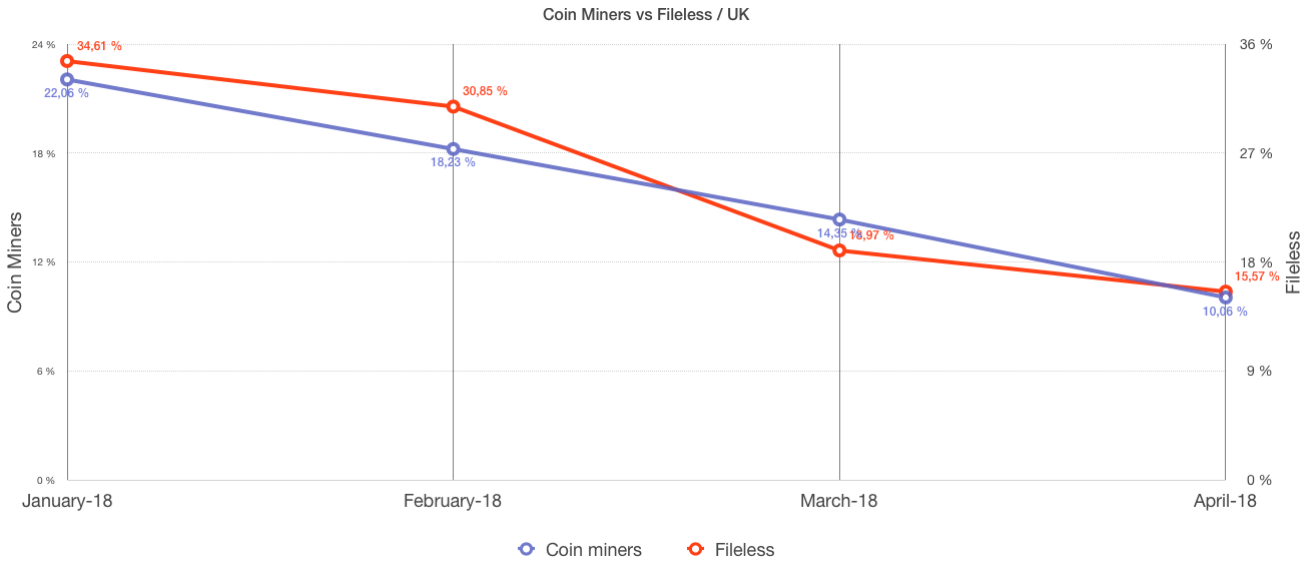

Fig. 6 – Fileless vs. Coin miners UK evolution

In the United Kingdom during the past four months (January through April 2018), coin miner and fileless reports dropped by **12 percent** of the total number of coin miner reports, and **19.04 percent** of the total number of ransomware reports (Fig. 6).

The same descending trend can be observed when analyzing the global evolution of the two (Fig. 7). Coin miner reports between January and April 18 have dropped from **22.48 percent** to **10.33 percent** of the total number of coin miner reports within that timeframe. At the same time, fileless dropped from January's **29.31 percent** to **19.86 percent** in April 2018, from the total amount of fileless reports in that timeframe.

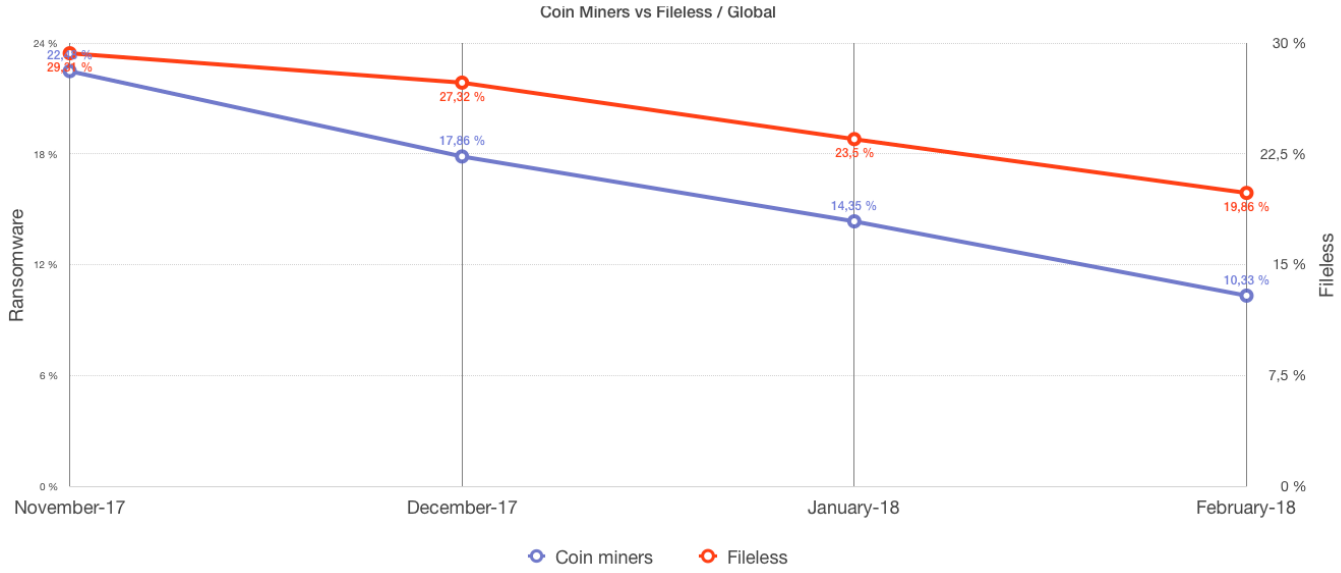

Fig. 7 – Coin Miners vs. Fileless global evolution

The Old, the New, the Money

Whether cybercriminals use ransomware or take advantage of the latest cryptocurrency craze, they'll stop at nothing when it comes to generating revenue. Ransomware has demonstrated unique abilities in terms of resilience and versatility, but recent cryptojacking campaigns have proven just as financially stimulating. However, threat actors have always shown remarkable ingenuity when it comes to leveraging even sophisticated threats, such as fileless techniques, and binding them together with something relatively benign, such as coin miners.

Cybercrime is all about money and exploiting the latest fad, the most advanced and stealth techniques, but even malware we've known about for years still manages to bag them serious revenue. If these recent stats about cryptojacking and fileless threats have taught us anything, it's that threat actors will use the most advanced tools at their disposal as long as the end goal is to quickly generate revenue, even if the payload is relatively benign.

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/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-May.25.2018-TK#: crea1826
Bitdefender-Whitepaper-infosec-crea2711-A4-en_EN