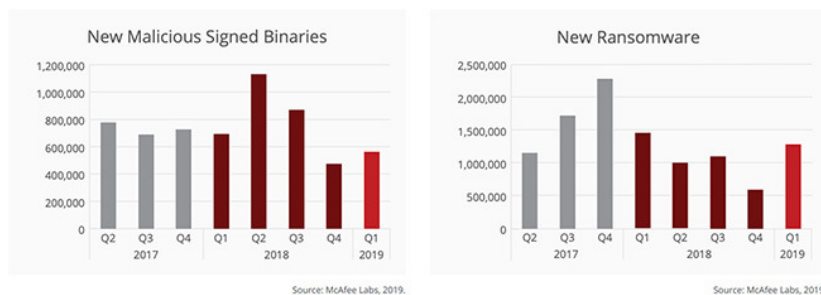


# New ransomware grows 118% as cybercriminals adopt fresh tactics and code innovations

Participate and win a drone: [Cybersecurity salary, skills, and stress survey](#)

McAfee Labs saw an average of 504 new threats per minute in Q1 2019, and a resurgence of **ransomware** along with changes in campaign execution and code. More than 2.2 billion stolen account credentials were made available on the cybercriminal underground over the course of the quarter. Sixty-eight percent of targeted attacks utilized spear-phishing for initial access, 77% relied upon user actions for campaign execution.



“The impact of these threats is very real,” said **Raj Samani**, McAfee fellow and chief scientist. “It’s important to recognize that the numbers, highlighting increases or decreases of certain types of attacks, only tell a fraction of the story. Every infection is another business dealing with outages, or a consumer facing major fraud. We must not forget for every cyberattack, there is a human cost.”

## Ransomware resurgence features new campaign tactics

McAfee Advanced Threat Research (ATR) observed innovations in ransomware campaigns, with shifts in initial access vectors, campaign management and technical innovations in the code.

While spear phishing remained popular, ransomware attacks increasingly targeted exposed remote access points, such as Remote Desktop Protocol (RDP); these credentials can be cracked through a brute-force attack or bought on the cybercriminal underground. RDP credentials can be used to gain admin privileges, granting full rights to distribute and execute malware on corporate networks.

McAfee researchers also **observed** actors behind ransomware attacks using anonymous email services to manage their campaigns versus the traditional approach of setting up command-and-control (C2) servers. Authorities and private partners often hunt for C2 servers to obtain decryption keys and create evasion tools. Thus, the use of email services is perceived by threat actors to be a more anonymous method of conducting criminal business.

The most active ransomware families of the quarter appeared to be Dharma (also known as Crysis), **GandCrab** and **Ryuk**. Other notable ransomware families of the quarter include Anatova, which was exposed by McAfee Advanced Threat Research before it had the opportunity to spread broadly, and Scarab, a persistent and prevalent ransomware family with regularly discovered new variants. Overall, new ransomware samples increased 118%.

“After a periodic decrease in new families and developments at the end of 2018, the first quarter of 2019 was game on again for ransomware, with code innovations and a new, much more targeted approach,” said **Christiaan Beek**, McAfee lead scientist and senior principal engineer. “Paying ransoms



Security pros need more and better visibility into their cloud networks

How to reduce the attack surface associated with medical devices

Google discovers websites exploiting iPhones, pushing spying implants en masse

CISO priorities: Implementing security from the get-go

Cybersecurity in the age of the remote workforce

**Spot light** **Whitepaper: Security Orchestration with Threat Intelligence**



Exabeam  
Cybersecurity  
Salary, Skills  
and Workplace  
Stress Survey

One participant will be randomly selected to win a DJI Phantom 3 Drone!

TAKE SURVEY

exabeam

## + What's New



What prevents companies from achieving effective security performance management?



Firefox now blocks third-party tracking cookies, cryptomining scripts by default



Security pros need more and better visibility into their cloud networks



A look into the frequency and success of phishing attacks on SMEs



How fraud prevention tech can save banks €10M a year



Free offering enables any MSP and security integrator to add incident response to their services portfolio



Researchers develop cheaper, more efficient