According to the Damballa Q2 State of Infections Report 18.5% of enterprise computers are "actively" communicated with criminals, while the past 18 months have seen a "dramatic" rise in ransomware.

When it comes to the numbers of infected machines, Dumballa says there is no correlation between size of enterprise and proportion of infected machines-- an enterprise with over 200000 machines might have a few infections, while a company with less than 600 devices may have a disproportionate amount of infection. In other words, company policies determine network cleanliness.

As for ransomware, Damballa reports a "sharp rise" in Kovter Ransomware infections, a form of police ransomware fraud first detected in 2013. June saw a peak in infections at 43713 known infected devices on a single day, and month-over-month daily infections increased by 153% in May and 52% in June.

"[M]anaging infections requires constant vigilance; advanced malware is designed to be evasive and threat actors are constantly seeking the next weakness to exploit," Damballa says. "Smaller organizations can have a very high ratio of infected devices and large enterprises can have low infection rates. It depends on the security controls in place. We recommend that security teams work under the assumption that prevention is not fail proof, so the ability to automatically detect and accelerate the time to response is essential to minimizing risk."

The report also mentions the success of Operation Tovar, a milestone in the coordination of law

enforcement and the wider security community in the takedown of the notorious GameoverZeus (GoZ) bonnet and its Cryptolocker payload. GoZ infected over 1 million devices worldwide and collected hundreds of millions of dollars in financial fraud, and while a new variant might appear Damballa and other researchers have observed a lack of immediate resurgence.

The full report is found in the link below.

Go Q2 State of Infections Report