Financial Sector

Safety and Soundness

The Situation

2019 has ushered in a historic crime wave in finance. Financial institutions are facing an evolving threat landscape. Fileless attacks and modular malware have been deployed widely across the financial sector supply chain. These attack vectors easily bypass traditional AV. This is compounded by the 160 percent increase of destructive attacks since 2018. The Bank heist has escalated to a hostage situation. The financial sector has long been the target of some of the world's greatest guilds of thieves however now nations states are targeting the sector to offset economic sanctions as evidenced by the North Korean and Russian indictments. The defense in depth architectures are failing due to the advent of SaaS, mobile banking and the migration to the cloud.

Over the past year, cyber defenders have observed dramatic innovation from cybercriminals, who are leveraging new tactics, techniques and procedures (TTPs) to maintain persistence, move laterally and leverage counter incident response efforts. It is imperative that financials institutions align their risk management strategy with the cognitive attack loop employed by these modern Dilinger gangs.

A Defensive Gameplan

Increase endpoint visibility

With the growing sophistication of attacks, CISOs need to look at any connected asset as a potential target. VMware Carbon Black's EPP empowers you to accelerate investigations and respond confidently to threats. Easy to digest attack chain visualizations—powered by real-time endpoint data—make it simple to see what has happened, and is happening, on your machines.

79 percent of surveyed financial institutions stated that cybercriminals are becoming more sophisticated

67 percent of surveyed financial institutions reported an increase in cyberattacks over the last year

72 percent of attacks on financial institutions are fileless in nature

37 percent of surveyed financial institutions have an established threat hunting team

Deploy endpoint detection and response (EDR)

Traditional antivirus solutions provide organizations with preventive protection—which can't protect from the full spectrum of attacks. Specifically, traditional AV is architected to look for indicators of compromise (IOC) associated with malware only. Fileless attacks are a blindspont for such solutions. VMware Carbon Black's EPP provides a more comprehensive solution that includes behavior intelligence, which is compulsory to detect living-off-the-land, fileless attacks. With this in place, security teams can continually collect, record, and store endpoint data, providing them with surveillance-like visibility that can be used to investigate a past incident or proactively hunt for threats.

Audit current system state

With the risk of attack ever present, it's important to audit your systems regularly and establishing remediation steps across all your security infrastructure. VMware Carbon Black's EPP allows you to query your endpoints, in real time, and at scale, with an intuitive and easy to use command line. This eases the burden of managing complexity for teams by making it simple to find vulnerabilities and to achieve (and prove) compliance.

LEARN MORE

To set up a personalized demo or try it free in your organization, visit *CarbonBlack.com/trial*

For more information or to purchase VMware Carbon Black Products please call: (855) 525-2489 in the US, (44) 118 908 2374 in EMEA

For more information, email *Contact@CarbonBlack.com* or visit *CarbonBlack.com*

vmware® Carbon Black