2019 has ushered in a historic crime wave in finance. Financial institutions (FIs) 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% 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 FIs align their risk management strategy with the cognitive attack loop employed by these modern Dilinger gangs.

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

72% of attacks on financial institutions are fileless in nature

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

Yet only 37% of surveyed financial institutions have an established threat hunting team
A DEFENSIVE GAMEPLAN

Increase Endpoint Visibility
With the growing sophistication of attacks, CISOs need to look at any connected asset as a potential target. 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.

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 blind spot for such solutions. 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. 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.

Integrate Your Security Controls
Without an integrated defense strategy, companies can’t achieve their strongest security. Organizations depend on multiple security products and when these products work together, they gain efficiency and speed. Carbon Black’s EPP offers open APIs which are used by more than 100 leading security product and service vendors to deliver seamlessly integrated solutions. These open APIs enable partners and customers the flexibility to custom-build their security stack with integrated solutions that amplify the investments they’ve made in Carbon Black and other security solutions.

Establish a Threat Hunting Team
Security teams struggle to obtain and access the endpoint data they need to investigate, and proactively hunt for, abnormal behavior. Many professionals currently lack the visibility to see beyond suspicious activity and need a way to dive deeper into the data to make their own judgments. Hunt-team exercises will empower CISOs with a game plan for increased safety and soundness thus empowering them within their FI with greater budget and authority.

Carbon Black’s EPP offers an advanced threat hunting and incident response solution. By leveraging unfiltered data, organizations have immediate access to the most complete picture of an attack at all times, reducing lengthy investigations from days to minutes. This empowers teams to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks and address gaps in defenses before attackers can.

To learn more about how Carbon Black can help secure your organization, contact us.
See: http://carbonblack.com/finance