The year 2020 will be one for cybersecurity defenders worldwide. Hackers, malicious actors and cybercriminals have seized the opportunity to exploit the security vulnerabilities exposed by the pandemic. Organizations shifted to distributed workforces almost overnight and now race to prepare their businesses for the future of work, the threat landscape has expanded, creating new, advanced threats for understaffed, overworked security teams.

The Ripple Effects of COVID-19

COVID-19 has changed the way we live, work, and we call external threats. In an unprecedented year, security professionals have faced the challenge of securing remote environments while small cybersecurity teams look to protect against the global disruption. On the frontline of security for their organizations, incident response (IR) professionals are grappling with advanced threat actors ranging from insider to outside hacking, lateral movement, destructive attacks and more.

The following findings are from the August 2020 Global Incident Response Threat Report by VMware Carbon Black. COVID-19 Continues to Create a Larger Surface Area for Cyberattacks. VMware Carbon Black surveyed IR professionals worldwide in April 2020. 52% of surveyed professionals who encountered or observed an increase in cyberattacks reporting against COVID-19 in April 2020, due to expedited challenges in:

- Increase in COVID-19 related malware uncovered in April 2020, according to surveyed IR professionals
- Remote access 52%
- VMware virtualization 45%
- VDI environments 36%

The average number of tools being used to manage security reported by surveyed cybersecurity leaders in March 2020: 8.91

CISOs are under more pressure than ever to keep their organizations secure. The pandemic accelerated digital transformation initiatives, including 5G adoption and cloud migration, creating new security challenges across organizations. The CISO’s role has become so integral they often now report directly to the CEO to ensure a cohesive security approach and help the C-suite and Board maintain customer trust as well as brand reputation.

A Look at the Evolving Threat Landscape Amid COVID-19

Financial institutions have long been targets for cybercrime syndicates,” said Tom Kellermann, Head of Cybersecurity Strategy, VMware Carbon Black. “Over the years, bank heists have escalated to virtual hostage situations where cybercriminals have seized the opportunity to exploit the security vulnerabilities exposed by the pandemic-fueled trends and threats identified by VMware Carbon Black experts this year. The following findings are from the third annual VMware Carbon Black Global Threat Report, which surveyed 3,012 CISOs, CTOs and CIOs in March 2020:

The average number of tools being used to manage security reported by surveyed cybersecurity leaders in March 2020: 8.91

89% of surveyed security leaders who state the volume of attacks they detected increased from October 2019 to March 2020

The following findings are from the August 2020 Global Incident Response Threat Report by VMware Carbon Black. COVID-19 Continues to Create a Larger Surface Area for Cyberattacks. VMware Carbon Black surveyed IR professionals worldwide in April 2020. 52% of surveyed professionals who encountered or observed an increase in cyberattacks reporting against COVID-19 in April 2020, due to expedited challenges in:

- Increase in COVID-19 related malware uncovered in April 2020, according to surveyed IR professionals
- Remote access 52%
- VMware virtualization 45%
- VDI environments 36%

92% of surveyed professionals who state the volume of attacks they detected increased from October 2019 to March 2020

The average number of tools being used to manage security reported by surveyed cybersecurity leaders in March 2020: 8.91

CISOs/CIOs that took part in the CISO/CIOs survey reported an increase in cyberattacks from February-April 2020, a 13% increase in April 2019 - April 2020, according to VMware Carbon Black. The increase of COVID-19 related malware uncovered in April 2020 was 95%

Remote access inefficiencies experienced between March 2019 - March 2020, has experienced between 135% - 238%

The average number of tools being used to manage security reported by surveyed cybersecurity leaders in March 2020: 8.91

The increase in COVID-19 related malware uncovered in April 2020, according to surveyed IR professionals was 95%

The average number of tools being used to manage security reported by surveyed cybersecurity leaders in March 2020: 8.91

CISOs/CIOs that took part in the CISO/CIOs survey reported an increase in cyberattacks from February-April 2020, a 13% increase in April 2019 - April 2020, according to VMware Carbon Black. The increase of COVID-19 related malware uncovered in April 2020 was 95%

Remote access inefficiencies experienced between March 2019 - March 2020, has experienced between 135% - 238%

The average number of tools being used to manage security reported by surveyed cybersecurity leaders in March 2020: 8.91

CISOs/CIOs that took part in the CISO/CIOs survey reported an increase in cyberattacks from February-April 2020, a 13% increase in April 2019 - April 2020, according to VMware Carbon Black. The increase of COVID-19 related malware uncovered in April 2020 was 95%