vmware® Carbon Black

A Look at the Evolving Threat Landscape Amid COVID-19

The year 2020 will live in infamy for cyber defenders worldwide. Hackers, malicious actors and cybercriminals have seized the opportunity to exploit the security vulnerabilities exposed by COVID-19. As organizations shifted to distributed workforces almost overnight and now look to prepare their businesses for the future of work, the threat landscape has expanded, creating new, advanced threats for understaffed, overworked security teams.

For Cybersecurity Awareness Month, here's a look at some of the biggest 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 CIOs, CTOs and CISOs in March 2020.

90%

Surveyed security leaders who state the volume of attacks they faced has increased from October 2019 to March 2020

91%

CIOs, CTOs and CISOs survey respondents who state that they had seen an increase in overall cyberattacks from October 2019 to March 2020 as a result of employees working from home

8.91

The average number of tools being used to manage security reported by surveyed cybersecurity leaders in March 2020, causing even more confusion

The Ripple Effects of COVID-19

COVID-19 has changed the way we live, work and how we combat cyberthreats. In an unprecedented year, security professionals are facing the challenge of securing remote endpoints while cybercriminals look to profit from the global disruption. On the frontline of security for their organizations, incident response (IR) professionals are grappling with exacerbated cyberthreats ranging from counter IR to island hopping, 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 49 IR professionals worldwide in April 2020.

53%: Surveyed IR professionals who encountered or observed an increase in cyberattacks exploiting COVID-19 in April 2020 due to endpoint challenges including:

52%

Remote access inefficiencies

45%

VPN vulnerabilities

36%

Staff shortages

92% The increase in COVID-19 related malware witnessed in April 2020, according to surveyed IR professionals

Spotlight on the CISO

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.

The following findings are from the third annual **VMware Carbon Black Global Threat Report**, which surveyed 3,012 CIOs, CTOs and CISOs in March 2020.

94%

CISOs/CIOs that took part in our research said they had suffered a data breach as a result of a cyberattack in the past 12 months, March 2019 - March 2020

2.17

The average number of breaches an organization has experienced between March 2019 - March 2020, according to surveyed security leaders

70%

Surveyed CISOs/CIOs who reported that they had suffered damage to their corporate image following a breach between March 2019 - March 2020

95%

CISO/CIOs survey respondents who were planning to adopt 5G over the coming year

Cashing in on COVID-19: The Focus on Finance

"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 cybercrime groups and nation-states have attempted to commandeer digital transformation efforts. Now, as we address the global impact of COVID-19, it's clear attackers are putting financial institutions directly in their crosshairs, according to our data."

The following findings are from the third annual VMware Carbon Black "**Modern Bank Heists**" report. The report combines original VMware Carbon Black threat data analysis with annual survey results featuring responses from 25 leading financial institution CISOs in April 2020.

238%

The increase of cyberattacks against the financial sector from February-April 2020, according to VMware Carbon Black threat data

80%

Surveyed banks reported an increase in cyberattacks from April 2019 - April 2020, a 13% increase over 2019

82%

Financial institutions who responded in our survey that cybercriminals have become more sophisticated from April 2019-April 2020, leveraging highly targeted social engineering attacks and advanced TTPs for hiding malicious activity

9X

The increase in ransomware attacks against the financial sector from February-April 2020, according to VMware Carbon Black threat data

Interested in learning more?
Check out our recent data reports **here** and learn more about the VMware Carbon Black Cloud solution **here**.