Introduction

Cybercrime is big business today—the World Economic Forum estimates its value at trillions of dollars each year¹ and characterizes its impact² as:

• Similar to that of a natural disaster
• Greater than that of a man-made environmental disaster—and more likely to happen

Among the factors driving the growth and impact of cybercrime are an unprecedented level of collaboration among nation states and increased cooperation among attackers generally.

Meanwhile, defensive technologies and approaches continuously improve, forcing attackers to become more organized and sophisticated, and make increased use of techniques like island hopping. We also expect cloud jacking to become more widespread as attackers target the cloud and hybrid infrastructures many organizations rely on today. And we anticipate a continued shift toward financial gain as the primary motivator of most attacks, with a parallel decline in focus on the theft of intellectual property (IP) and customer information.

Trend 1.
More Attacks Will Use Island Hopping and Lateral Movement

We’re seeing attackers making more use of island hopping and lateral movement, trends that look set to go on increasing.

Island hopping is on the rise because hackers know better than to directly attack a well-defended target. Instead, the attacker looks to gain access to the target organization via a smaller third party that works with the target and may be less protected.

The increasing number of third parties—such as remote employees, contractors, law firms and marketing firms—that typically connect to enterprise networks today gives attackers plenty of island-hopping options to exploit. Attackers who cloud jack or purchase access to compromised infrastructure often do so for the purpose of island hopping.

Once inside the target environment, attackers will often move laterally rather than in a linear fashion. In particular, if they don’t reach their goal directly, they’ll pivot to try something else and approach it via a different route.

---

Trend 2.
Cloud Jacking Will Become Commonplace

Cloud jacking—also called hyper jacking—will become a more common practice as attackers look to exploit the cloud and hybrid infrastructures that organizations increasingly adopt.

Cloud jacking involves an attacker taking malicious control over the hypervisor (or installing a fake hypervisor) that manages the entire server system. The attacker may be a malicious outsider but equally may be a trusted third party involved in managing the organization’s infrastructure.

A successful cloud-jacking attack enables the attacker to affect the operation of the targeted organization. We’re also seeing an increase in cloud-jacking attacks as the precursor to island hopping (see Trend 1). In these cases, the attacker cloud jacks an organization that’s connected to their real target, then uses the compromised organization as a stepping stone to penetrate it.
Trend 3. The Nature of Mobile Attacks Will Evolve

The vulnerability of mobile devices, and the data they allow users to access anytime, anywhere, will likely continue to be a major concern for CISOs.

Until recently, attacks on mobile devices tended to enable criminal activities, such as click jacking (or phishing) and cryptomining (diverting the device’s resources toward cryptocurrency mining).

During 2020 and beyond, however, we anticipate increased use of mobile rootkits to take control of a user’s mobile device, with these attacks carried out by nation states, organized crime syndicates, terrorist groups and others.4 If the attack is successful, the attacker can then become persistent in the user’s physical environment, and carry out virtual snooping, stalking or spying via the compromised mobile device.

Trend 4.
Access Mining as a Service Will Expand

The business model for access mining combines two profit streams:

- Cryptomining, which uses the resources of a compromised computer, smartphone or other device for cryptocurrency mining
- Sales of system access to organized crime syndicates, nation states or the compromised entity’s competitors

Just like any other form of attack, access mining is being turned into a service. Starting in 2020, we expect to see a significant increase in access mining-as-a-service offerings on the dark web as more and more bad actors move to take advantage of this highly lucrative type of cybercrime.
Trend 5. Use of Custom Malware Will Keep Increasing

While the use of commodity malware declined slightly during the course of 2019, custom malware was used in 41 percent of attacks in the final quarter, up from 33 percent in the first quarter.5

Custom malware is malware developed for specific target environments. Like many other types of attack, custom malware is increasingly becoming available as a service on the dark web, and therefore usable by individuals with no knowledge of coding.

Increasingly, developers of custom malware look beyond simply selling their service for profit. When a buyer uses custom malware to breach a target environment, they open a backdoor for the original developer, who can use remote administrator access to carry out their own attacks on the target in the future.

WHAT IS CUSTOM MALWARE?
The term “custom malware” describes fileless attacks, pieces of code or scripts that leverage existing and legitimate software to execute. Often, custom malware appears as an unknown file whose malicious intent is discovered only when executed.

Trend 6.
Public Figures Will Continue to Be Hit by Attacks on Smart Devices

In today’s connected homes, cameras, speakers, thermostats and other smart devices connect and work alongside each other on the Internet of Things (IoT), and are integrated into our everyday lives. However, these devices often lack the required security protection, leaving them vulnerable to attack.

A smart device attack (or virtual home invasion) can be devastating for anyone, but when carried out against a public figure—such as a celebrity, politician or CEO—the aims and consequences of such an attack can be even more serious. The fact that their smart home infrastructure provides connections to other high-profile individuals—or access to restricted systems and valuable data—makes these figures a target for hackers intent on blackmail, extortion or corporate espionage.

As adoption of smart technology and IoT devices continues, and working from home increasingly becomes the norm, we anticipate a dramatic uptick in these attacks.6

---

Trend 7. 
Attacks of a Destructive Nature Will Continue to Rise

Incident response (IR) professionals reported experiencing destructive attacks in about 41 percent of cases during the last quarter of 2019. That’s a 10 percent increase on the previous two quarters and an ominous upward trend.

IR professionals report two reasons for this increase:

• A significant rise in geopolitical tension

• Adversaries becoming aware of defensive measures

Going forward, we also expect to see a rise in a more sophisticated type of destructive attack: integrity attacks that involve adversaries doing anything from changing entries in a database to manipulating time in the compromised infrastructure. For the target of the attack, identifying exactly what was changed and when can be a challenging, time-consuming and costly process.

We anticipate that integrity attacks will pose a growing risk to political processes worldwide (see Trend 10).

Trend 8. Financial Gain Will Remain the Primary Motivation for Attacks

Financial gain was the primary motivation for 90 percent of cyberattacks in the second half of 2019.8 That was a sharp increase from 61 percent in the first six months of the year and part of the ongoing shift away from a time when the theft of IP and customer information topped the list.

Interestingly, we observe that the nature of financially motivated attacks is changing. Traditionally, the focus has been on moving money via wire transfer fraud and other similar techniques. But more sophisticated cyber crews are now looking to acquire non-public market information that enables them to conduct digital front running or digital insider trading to benefit their portfolios.

We anticipate this shift will continue as more crews learn that gaining intelligence to use in the markets will yield far greater gains than simply breaking into bank accounts.

---

Trend 9.
Nation States Will Continue to Use Cyberattacks to Maintain Market Leadership

Statistically, hackers in China, Russia and the U.S. were responsible for the lion’s share of cyberattacks in 2019, and there’s no sign of this changing in the short or medium term.

Motivation can be related to a desire to maintain market leadership in sectors, such as technology. Geopolitical power and increased tension between the world’s most powerful states are additional major contributing factors.

As political situations continue to change, China and other rogue states are accelerating the development of advanced cyberattack capabilities.

Which countries account for the most attacks?
When asked this question in 2019, IR professionals said:

- Russia: 29%
- China: 18%
- United States: 11%
- North Korea: 4%

Trend 10.
Concerns Will Persist Around Worldwide Political Processes, Risk and Security

Despite extensive work to protect political processes and campaigns, and to harden voting systems, it’s difficult to control layer 8—the human element. Voters in any election, poll or referendum in any country can be manipulated by waves of disinformation and sophisticated deep fakes and news bots released by rival groups, nation states and others determined to exert a malign influence on the democratic process.

Alongside voter manipulation activities, we expect to see an increase in integrity attacks on voter databases during 2020. The aim of these attacks will be to disenfranchise or suppress voters based on factors—such as affiliation, locality or ethnicity—to directly affect the outcome of a political process by controlling who is able to vote.
Conclusion

With little evidence of improvements in the geopolitical situation, we expect to see a continued rise in attacks by nation states alongside those carried out by organized crime syndicates, terrorist groups and others.

The plethora of advanced hacking capabilities and services for sale on the dark web means that almost anyone can launch a cyberattack, with no coding skills required. The most skilled hackers are focusing on developing highly customized malware for sale. In addition to immediate financial gain, sales of custom malware put them in a strong position for future access to environments compromised by their code.

Despite growth in attack numbers and sophistication, it’s actually a great time to be a defender. There’s more—and more capable—technology available to support defenders in their efforts than ever before. On top of that, there’s a great deal more collaboration among the defender community and increased sharing of information about attackers’ tactics, techniques and procedures (TTP). All of which empowers defenders to gain ground against even the most determined adversary.

Here at VMware, we’re dedicated to keeping the world safe from cyberattacks. Our cloud native security platform uses big data and behavioral analytics to protect endpoints and workloads against sophisticated attacks and enable rapid response. We help customers build a digital foundation with intrinsic security that protects any app, running on any cloud, delivered to any device.

Contact us to request a personalized demo of VMware Carbon Black security capabilities.
About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit vmware.com/company.

Join us online: