Global Incident Response Threat Report

The Cybersecurity Tipping Point: Election, COVID-19 create perfect storm for increasingly sophisticated cyberattacks

As eCrime groups grow more powerful, counter incident response now seen in 82 percent of attacks—with island hopping occurring 55 percent of the time

Tom Kellermann, Head of Cybersecurity Strategy
Greg Foss, Senior Cybersecurity Strategist

October 2020

GET STARTED

vmware® Carbon Black

Executive summary

"Criminals never let a good crisis go to waste," observes Greg Foss, senior cybersecurity strategist at VMware Carbon Black.

This certainly holds true amid the COVID-19 pandemic. In April 2020, the FBI and Secret Service reported a wave of COVID-19-related cybercrimes and threats as criminals capitalized on widespread anxiety, confusion and reliance on digital technology and online networks.[1]

As November approaches, the cybersecurity challenges of the pandemic are colliding with the 2020 U.S. presidential election. According to the Cybersecurity and Infrastructure Security Agency (CISA), the "threat landscape is constantly evolving, and dedicated, malicious actors with virtually unlimited resources will always be able to penetrate some aspect of American networks"[2] ahead of the election. Cybersecurity has already begun to take on new urgency as government entities used by election officials or with relevant voter data are hit with ransomware attacks.[3]

This concurs with findings in our sixth Global Incident Response Threat Report, wherein nearly half (49 percent) of cybersecurity professionals named government as the industry most targeted by attacks; media and entertainment, which can also be leveraged for election-related hacks, was named by 42 percent of respondents. These percentages are roughly double the findings in our August report.[4]

Even more troubling, however, is that today's cyberattacks—pandemic-related, election-related or otherwise—have grown increasingly sophisticated and destructive. In our latest survey, respondents reported that 82 percent of attacks now involve instances of counter incident response (IR), and 55 percent involve island hopping, where an attacker infiltrates an organization's network to launch attacks on others along its supply chain. This represents a significant surge since our August report, where only 33 percent of attacks involved counter.[4]

For Tom Kellermann, head of cybersecurity strategy at VMware Carbon Black, the recent findings suggest a significant renaissance in cybercrime, which he believes is leading to a new era of agile organization and sophistication.

"The disruption caused by COVID-19 has created a massive opportunity for criminals to restructure their businesses," he says. "Traditional criminals are flocking online in a newly shifted digital-first world, fueling the expansion of cybercriminal cartels."

These forces, combined with the scale of the dark web (the World Economic Forum predicts it will become the third largest economy by 2021),[5] now pose new security challenges for IR and cybersecurity professionals responsible for detecting and stopping emerging attacks.

In what follows, we'll paint a picture of this evolving threat landscape by discussing the impact of COVID-19 and the U.S. presidential election and providing some best practices for IR teams and security teams looking to fight back. The survey findings—drawing on responses from 83 cybersecurity professionals—build on previous iterations of the Global Incident Response Threat Report, of which this is the sixth.

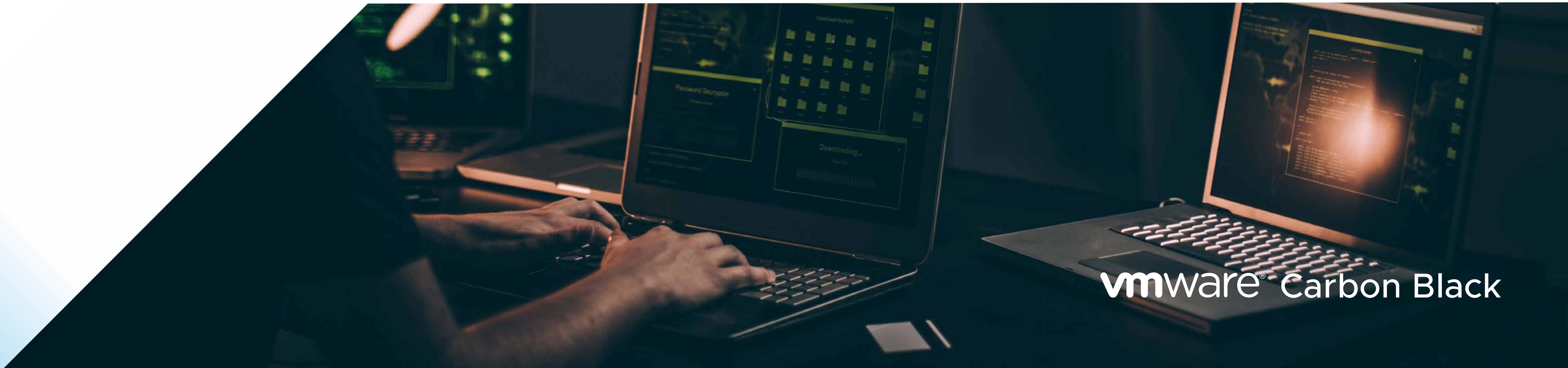
Key findings

Incidents of counter IR are at an all-time high, occurring in 82 percent of IR engagements—suggesting the prevalence of increasingly sophisticated, often nation-state attackers, who have the resources and cyber savvy to colonize victims' networks. Destructive attacks, which are often the final stage of counter IR have also surged, with respondents estimating victims experience them 54 percent of the time.

55 percent of cyberattacks target the victim's digital infrastructure for the purpose of island hopping. The pandemic has left organizations increasingly vulnerable to such attacks as their employees shift to remote work—and less secure home networks and devices.

Custom malware is now being used in 50 percent of the attacks reported by respondents demonstrating the scale of the dark web, where such malware and malware services can be purchased to empower traditional criminals, spies and terrorists, many of whom do not have the sophisticated resources to execute these attacks.

As we approach the presidential election cybersecurity remains a top concern and nation-state attackers pose a significant threat. Drawing upon their security expertise—and in line with recent advisories from CISA[6]—73 percent of respondents believe there will be foreign influence on the 2020 presidential election, and 60 percent believe it will be influenced by a cyberattack. When asked which countries could be the source of such attempts, IR and cybersecurity professionals named Russia (58 percent), North Korea (27 percent) and Iran (19 percent).



vmware® Carbon Black

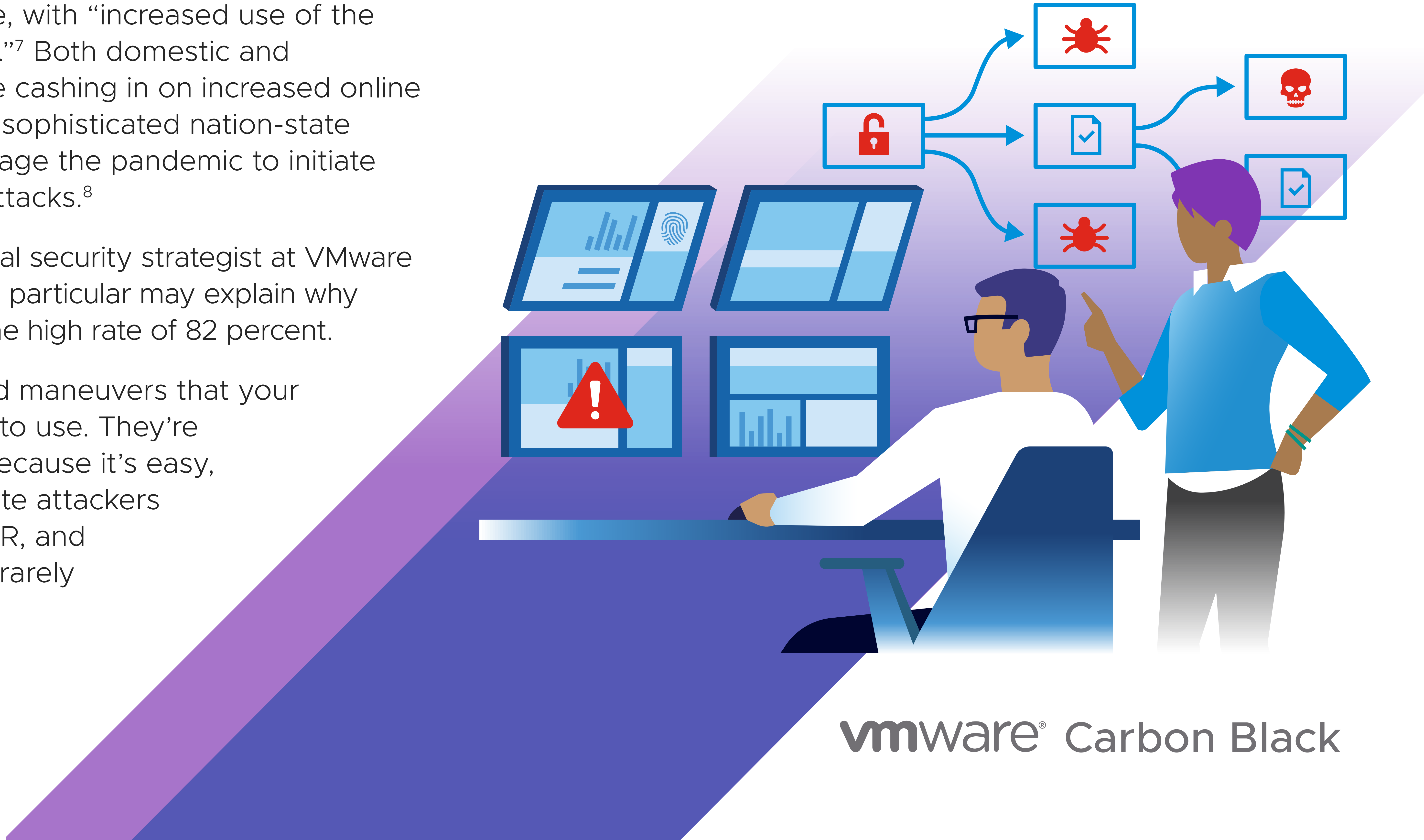
An increasingly sophisticated—and destructive—threat landscape

The pandemic, which for many organizations meant a rapid shift to remote work, has expanded the corporate perimeters into employees' homes—and catalyzed the development of a dangerous new threat landscape.

As a result, security/IT staff are so overworked that nearly a third (28 percent) of respondents see this as the biggest challenge to effective IR. There's also the evolution of traditional criminality to eCrime, with "increased use of the dark web for criminal activities."[7] Both domestic and international cybercriminals are cashing in on increased online activity due to COVID-19,[7] and sophisticated nation-state actors have been able to leverage the pandemic to initiate malicious malware and cyberattacks.[8]

According to Eric O'Neill, national security strategist at VMware Carbon Black, the latter point in particular may explain why respondents reported an all-time high rate of 82 percent.

"These are highly sophisticated maneuvers that your typical criminal just isn't going to use. They're going to use spear phishing, because it's easy, and it works. It's the nation-state attackers that are often behind counter IR, and Western law enforcement has rarely been able to stop them."



Counter IR takes several forms, including:

- Disabling Application Solution Module (ASM)
- Clearing/deleting logs
- Manipulating time stamps
- Using alternative authentication
- Signed binary proxy execution
- Rootkits
- Disabling security tools
- Virtualization and/or sandbox evasion
- Masquerading
- Software packing
- Data obfuscation

vmware® Carbon Black

Where have the majority of attacks you deal with during IR engagements originated?

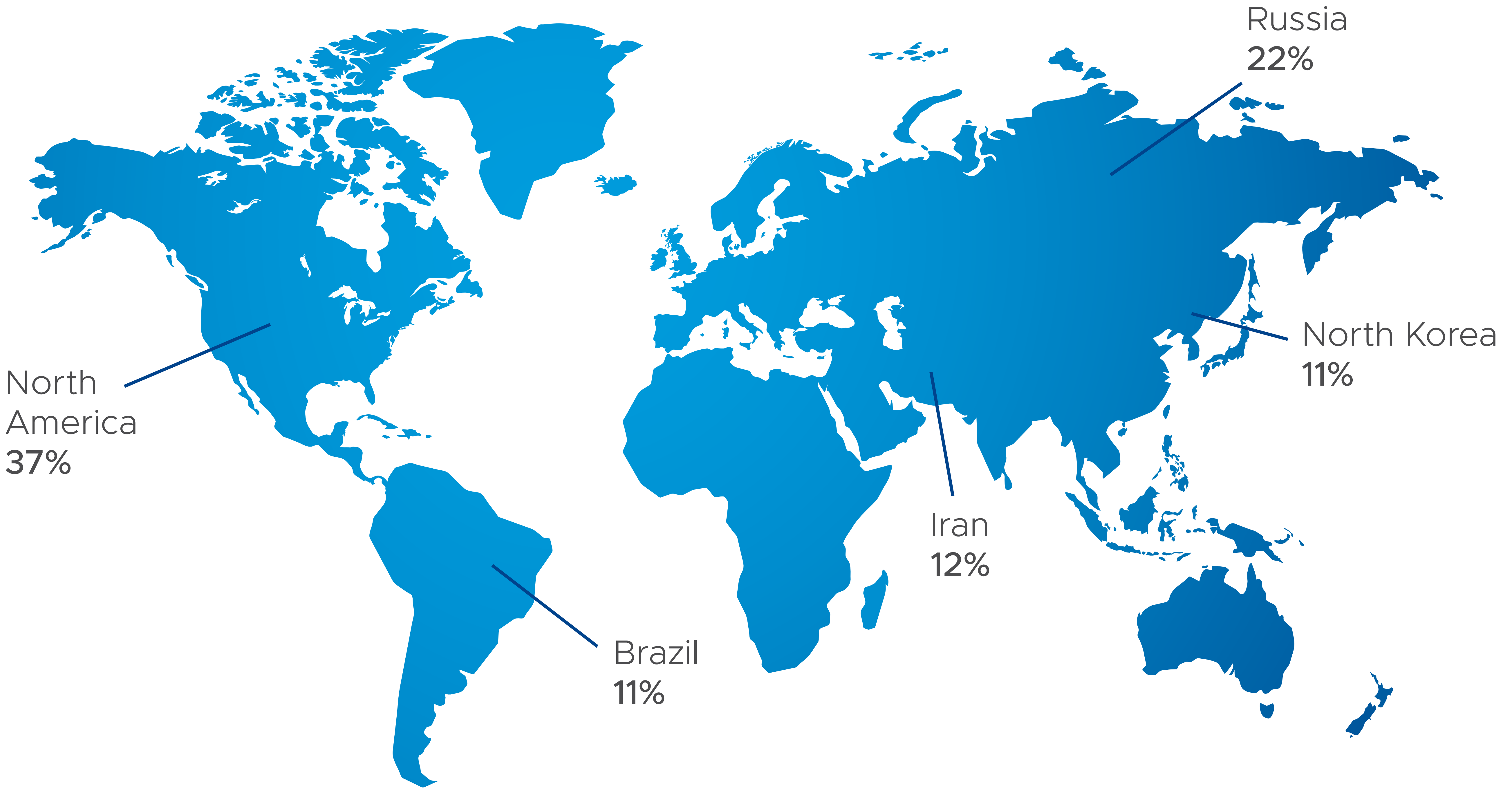


FIGURE 1: Multiple answers per participant possible. Percentages added may exceed 100 since a participant may select more than one answer for this question.

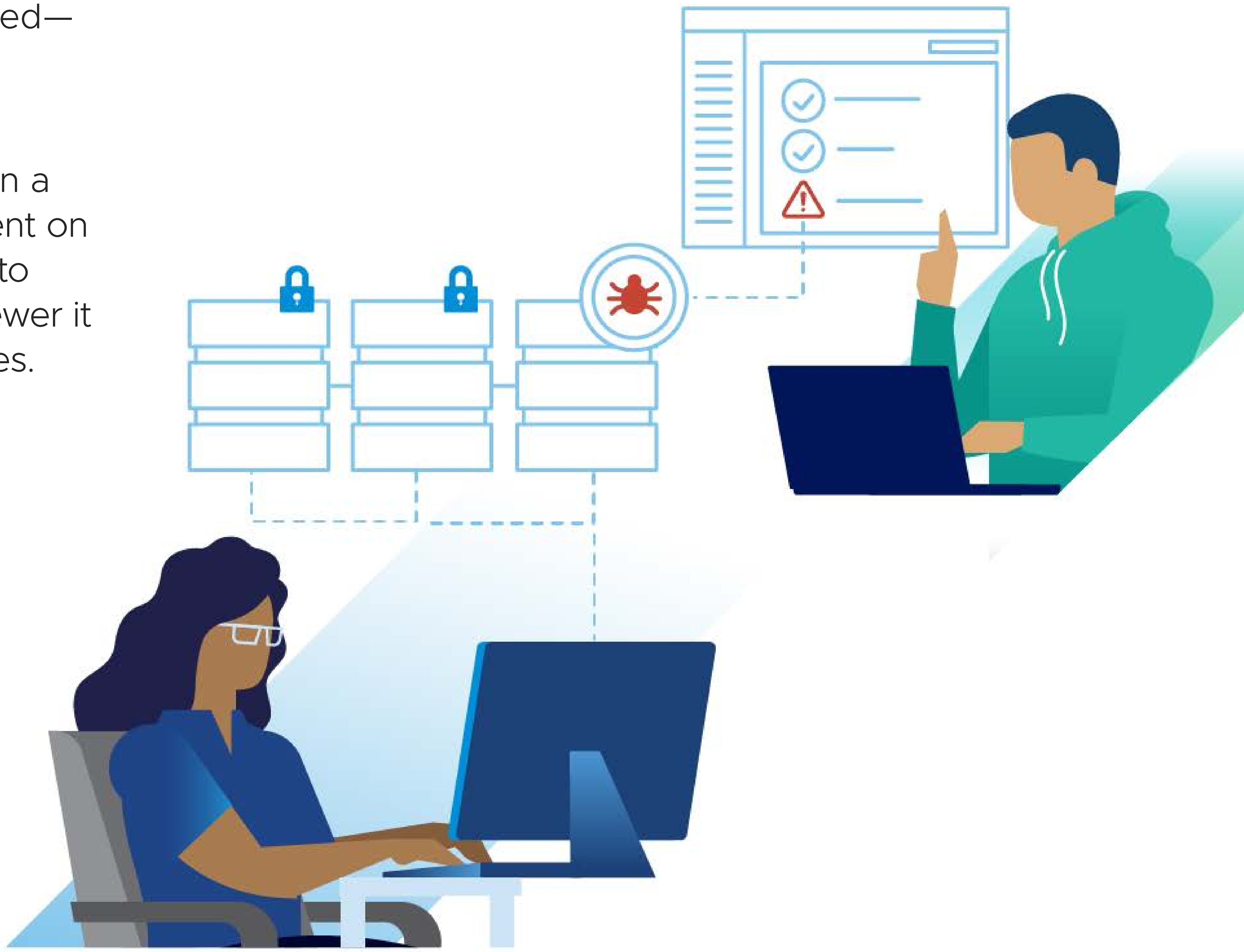
These counter IR techniques are largely facilitated by lateral movement—estimated to occur in more than 62 percent of attacks—which in turn facilitates island hopping, seen by respondents in 55 percent of IR engagements. According to Kellermann, the significant percentage (37 percent) of attacks noted in the survey as originating from North America is a smokescreen, as island hopping attacks may look like they're coming from the U.S. when in actuality they are originating from compromised U.S. infrastructure. This is evidenced by the increased sophistication of attacks and the continued urgency in federal government alerts warning of new threats and vulnerabilities.[9]

"For these criminal groups, there is a desire is to create a renaissance," Kellermann says. "Lateral movement is metastasizing into island hopping, through an organization's website, applications, mail server, email. It's colonization. What used to be a burglary has now become a home invasion."

Another tactic in this effort involves using secondary command and control (C2) on a sleep cycle, which respondents are now seeing in approximately 66 percent of attacks. This allows criminals to regain access even if their main entry point is outed—oftentimes without defenders knowing about it.

Foss notes that command and control has been leveraged in attacks on celebrity social media profiles to control malware in a clandestine fashion.[10] Because so many people publicly comment on celebrity Instagram photos, for example, it's easy for attackers to post commands from an individual's profile. While to the lay viewer it may not be obvious, malware can read and execute these codes.

"It allows hackers to maintain command and control on their host without leaving an obvious trail," he says. "It just looks like they're using social media. It's great for lateral movement and pivoting to other hosts. This is why tying process data to network activity is such a key component of threat hunting."



Which dual purpose tools help facilitate lateral movement for attackers?

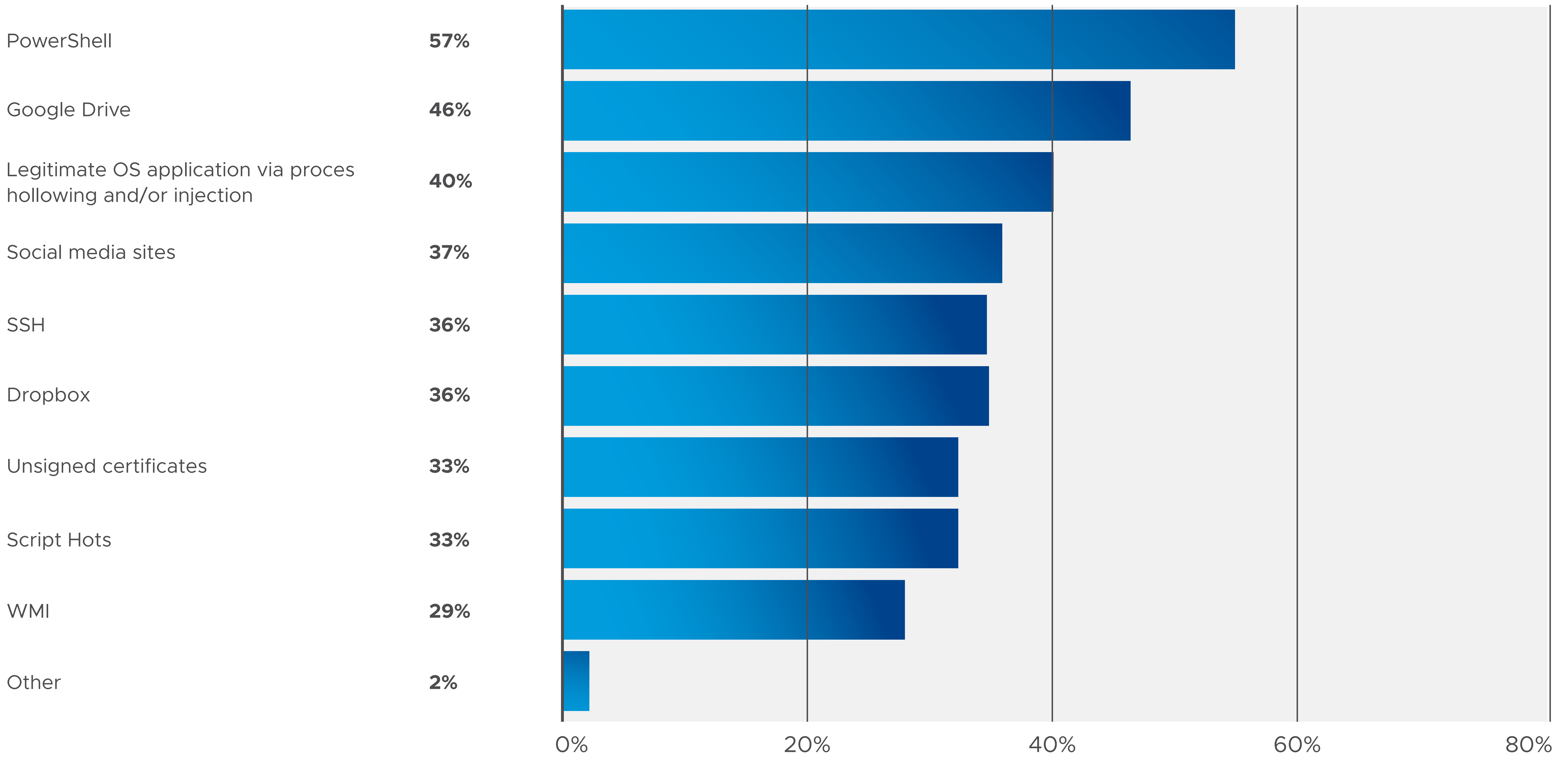


FIGURE 2: Multiple answers per participant possible. Percentages added may exceed 100 since a participant may select more than one answer for this question.

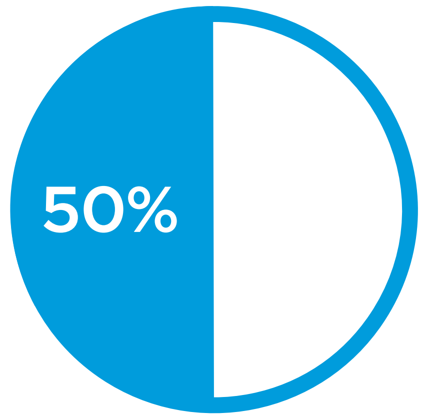
It should come as no surprise that the use of social media sites that the use of social media sites to facilitate lateral movement was seen by more respondents (37 percent) than ever before in this report. The same was true of Google Drive (46 percent), which points to the shift to work-from-home and the increased use of the application for remote learning contexts. Foss adds, “In customer IR cases, we are also seeing ransomware double-extortion groups leverage open source technology solutions like ownCloud to exfiltrate sensitive data from target networks.”

Ultimately, the final stage of these increasingly sophisticated attacks often ends in destructive actions, be it a denial of service, ransomware, multifunctional wipers (i.e., repurposed ransomware that makes it impossible to recover encrypted data) or hybrid attacks that start in cyberspace but involve physical destruction, among others.

eCrime groups, the dark web and the rise of ransomware as a service

“We like to think of cyberattacks as being the work of an individual hacker sitting in the basement,” says O’Neill. “But there’s actually a large business behind it, an entire infrastructure.”

And this infrastructure is selling access and malware on the dark web to anyone with money to burn by way of initial access brokers. It goes a long way toward explaining the rise in island hopping (i.e., via resold access), the fact that respondents are experiencing custom malware in 50 percent of attacks and why 55 percent of respondents say the use of ransomware increased at the start of the pandemic.



Custom malware is now seen in 50 percent of engagements, and why 55 percent of respondents say the use of ransomware has increased the start of the pandemic.

“We’re seeing a significant increase of new and improved ransomware as a service,” Foss says. “If you have enough money, you can purchase access to an impacted organization without needing much hacking skill. The combination of initial access brokers and ransomware as a service has really lowered the bar of entry into this space for cybercriminals.”

The use of ransomware by powerful eCrime groups has also evolved: from a simple money grab to wholesale extortion, as observed by VMware Carbon Black threat researchers on the dark web. “Cybercriminals are advancing activity beyond the expected phishing emails,” Foss notes. “Now, as CISA has warned, they’re taking time to fully understand and map out the business from the inside and exfiltrating sensitive data before encrypting.”[11]

The Maze cartel, which is believed to be comprised of more than 150 members—and which continues to grow by partnering with other prominent ransomware groups—offers a prime example.[12] The group moves through a network manually, covertly, looking to understand an organization’s infrastructure and exfiltrate sensitive data; and ultimately, if the host doesn’t pay the ransom, they use that data against them, publicly exposing their most sensitive content online for the world to see.

Unfortunately, these moves don’t look to be slowing down anytime soon. “The bottom line is that it’s lucrative,” O’Neill says. In fact, the FBI revealed that more than $140 million was paid in ransoms between 2013 and 2019.[13]

How to fight back: New best practices for threat hunting

"The nature of today's attacks—namely, the rise in counter IR (82 percent), custom malware (50 percent) and island hopping (55 percent) observed by respondents—is shifting how the cybersecurity industry conducts IR," says Kellermann. "Nowadays, if you turn on the lights on an attacker, you're going to be dealing with an escalation."

So, what tactics and principles should IR professionals keep top of mind? Here are five new best practices to stay one step ahead of attackers:

1. **When discussing an intrusion, set up secure communication channels.** Today's attackers will often attempt to monitor communications—especially those of the security team. For Foss, that means "the first and arguably most important step is to set up out-of-bands communication channels so that you can discuss and share information without giving away that you are actively looking into their activities."
2. **Assume the adversary has multiple avenues back into the organization.** Resisting the urge to shut them out will pay dividends in the long run. Be patient, wait, watch, learn and only strike when you are reasonably sure about the scope and breadth of the intrusion.
3. **To combat alert fatigue, baseline your organization.** Overworked security teams are using tools to detect more than ever; yet doing so can overwhelm these teams even more, while drowning out what's important. To amend this, Foss suggests an organization map out where their most important assets lie—and then build out controls and tune security systems around those priorities. From there, security teams can begin a broader inventory management process, bucketing certain assets into logical groupings for more effective IR.
4. **Build the capacity to detect and respond across workloads.** "In the transition to a remote, cloud-run working environment," Kellermann says, "workload security is imperative. Otherwise these environments become a one-stop shop for island hopping and other methods to commandeer the network." This means protecting cloud environments, containers and microservices where most of the work is happening nowadays—the applications that exist between a system's networks and its endpoints.
5. **Segment personal and professional networks.** Amid COVID-19 the corporate perimeter has expanded in employee homes, ushering in a deluge of new attacks on home routers and networks, which is only made more challenging with the lack of visibility security professionals have into those networks (especially while they, too, work from home).

“In our work with IR partners, one of the most successful results was with a customer who had specific rules based on different organizational units within the company,” Foss explains. “For instance, if an engineer or IT staff member used command line arguments like ‘whoami,’ it wouldn’t raise as many eyebrows as if that command was executed from an HR employee’s system. This allowed them to spot an anomaly and catch an intrusion fast. But setting up security tools this way takes time and effort to do properly. That’s the hard work.”

What is the biggest challenge to effective incident response as a result of remote work conditions?

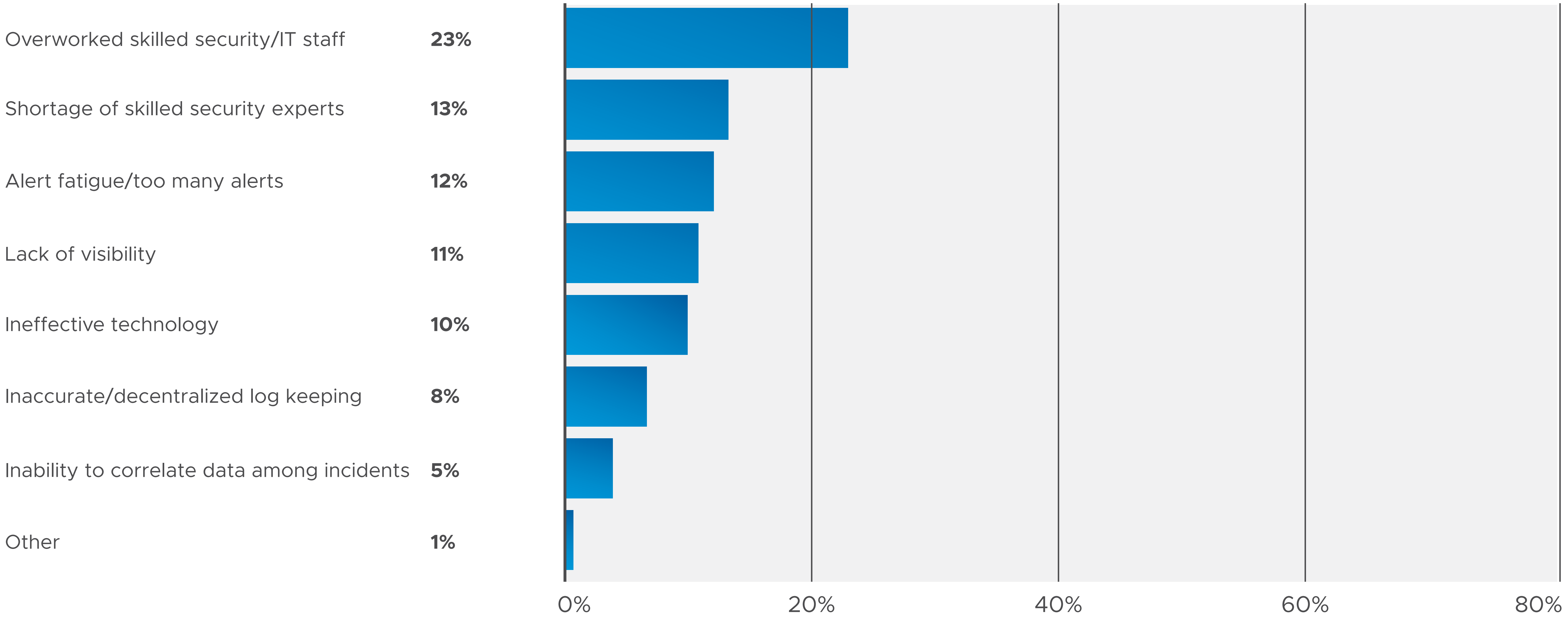


FIGURE 3: Multiple answers per participant possible. Percentages added may exceed 100 since a participant may select more than one answer for this question.

2020 election security: what security pros are saying about cyberattacks, foreign influence and more

Cybersecurity has become a critical concern ahead of the 2020 U.S. presidential election.[14] In an unprecedented year, we have already begun to see foreign interference,[15] government agencies hit with ransomware attacks[16] and more. This is all compounded by the pandemic, which has created logistical challenges and complicated access to voting.[17]

Drawing upon their security expertise, survey respondents weighed in on election security and trends they are watching. For instance, as cyberattackers up their game, 64 percent said the 2020 presidential election is at more risk than four years ago—with half (32 percent) saying that risk has increased by a significant amount. When asked which nation-state actors they expect to be a source of hacking attempts to the election, IR and cybersecurity professionals named Russia (58 percent), North Korea (27 percent) and Iran (19 percent); 73 percent of respondents believe there will be foreign influence on the election.

Which of the following countries do you expect to be the source of the hacking attempts during the 2020 election?

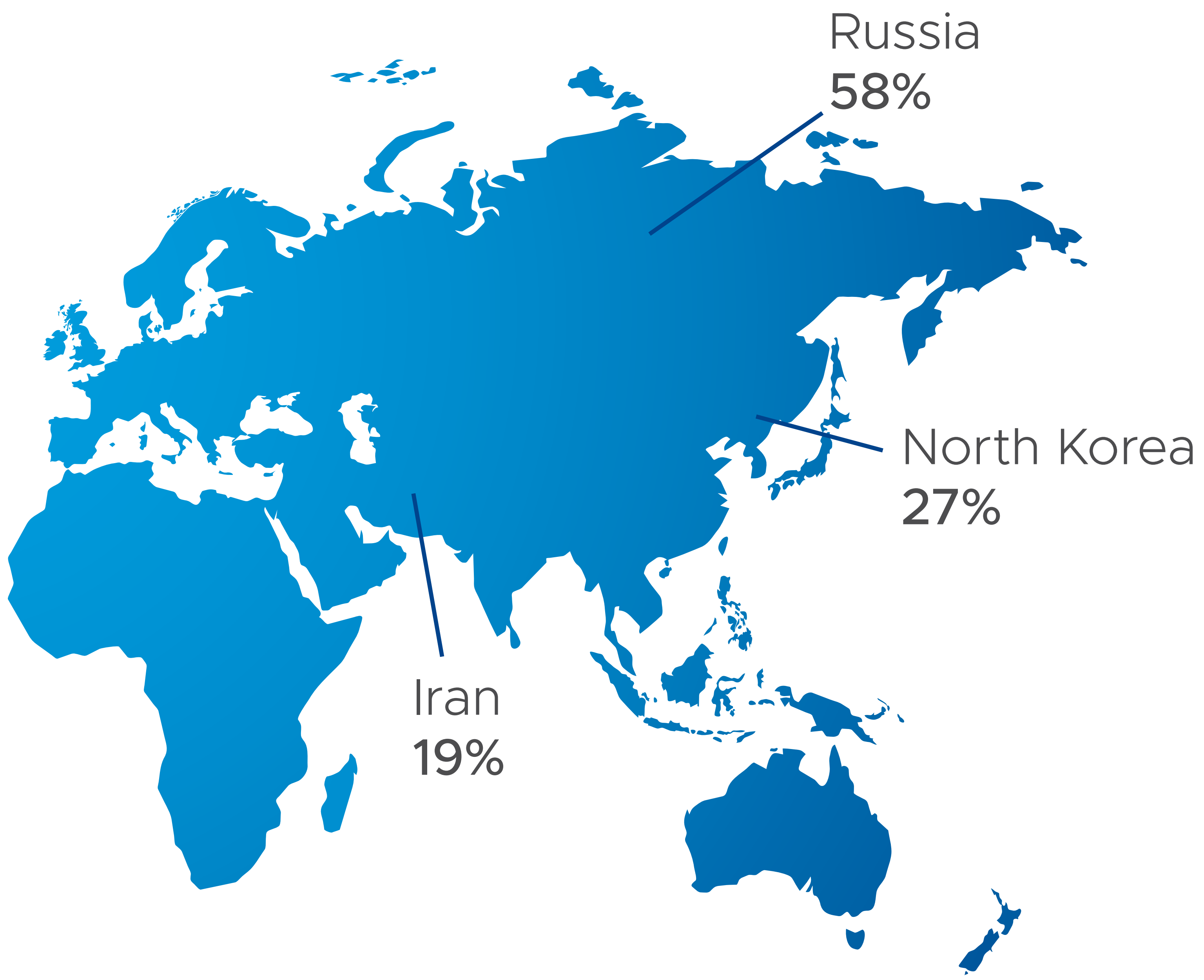


FIGURE 4: Multiple answers per participant possible. Percentages added may exceed 100 since a participant may select more than one answer for this question.

In a joint cybersecurity advisory, CISA and the FBI reported advanced persistent threat (APT) actors targeting election organizations, data and support systems.[18] Our respondents concur: when asked about the greatest election security risks, their top three responses were election official databases, voter registration and voting machines.

For O'Neill, securing voting infrastructure should be the primary focus. "If you haven't designed it from the ground up, hackers will find a vulnerability to attack," he says.

To bolster cyber defense, respondents thought strong passwords (including multi-factor authentication), securing voting infrastructure and endpoint controls should be prioritized.

This concerning threat landscape means it's time that state and local governments rethink cybersecurity. In the VMware Carbon Black whitepaper *Best Practices for Securing Critical Infrastructure for State and Local Governments*,[19] we highlight additional measures agencies can use to stay better secure, as well as some possible consequences of leaving vulnerabilities unaddressed.

The biggest cybersecurity threats to the 2020 election and how to fight back

There are multiple ways for bad actors to disrupt the election process, the most concerning of which—according to our respondents—include misinformation/disinformation (27 percent), ransomware (20 percent), voter manipulation or fraud (20 percent), and voter disenfranchisement via an integrity attack on rolls (18 percent).

With these cybersecurity threats looming, what tools can help secure the vote? Here are four best practices to stay one step ahead of attackers:

1. **Disinformation on social media.** During the 2016 presidential election, Russian operatives used Facebook, Instagram, Twitter and other social media platforms to spread disinformation—and these targeted campaigns have continued. In September of this year, for instance, the FBI and CISA released a warning[20] alerting the public about the potential for widespread disinformation campaigns designed to cast doubt about the legitimacy of the November elections.

Cyber defense: Today, no specific tools exist to address this issue. Thus to fight now-rampant disinformation campaigns, social media platforms will need to develop these tools themselves, or codevelop them with security vendors who can help build them into their platforms.

2. **Ransomware attacks.** In the first two weeks of September alone, seven government entities were hit by ransomware and had their data stolen.[21] These attacks can jeopardize the integrity of the election by giving voters the impression that their vote will not be accurately counted or attacks have compromised voting systems.

Cyber defense: When it comes to the actual infrastructure (servers, workstations, voting machines running on Windows/Linux), security teams should implement next-generation antivirus software. Email security should include attachment detonation, Secure Access Server Edge (SASE), web application firewall, and network detection and response (NDR) to reduce the likelihood of the attack being delivered and internally spread.

3. **Vote manipulation.** Last year, a group of white hat hackers[21] proved that machines used in more than half of the United States in 2018 were vulnerable to hacking[22]—a vulnerability which remains in 2020. The possibility for vote manipulation is very real.

Cyber defense: Primarily, voting machines need endpoint and cloud workforce protection platforms (EPP and CWPP) in place. As a backstop, SASE and NDR should be baked into North-South traffic (client to server), internal traffic, and software-defined networking in a wide area network (SD-WAN).

4. **Voter disenfranchisement.** Voter registration systems and databases are managed on a state-to-state basis and often built on unsecured technology—making them a prime target for hackers..

Cyber defense: Ssimilar to securing against attacks on vote manipulation, EPP and CWPP primarily, with SASE and NDR (baked into North-South, SD-WAN, internal) as backstop.

Navigating the storm

Cybersecurity is now at a tipping point as the threat landscape continues to evolve with increasingly sophisticated cyberattacks—cyberattacks brought on, in large part, by the collision of COVID-19, the U.S. presidential election and the growing threat of cybercriminal groups.

But while global disruptions might be an opportunity for criminals, they're also an opportunity for those who defend against attacks to rethink security postures and fight back.

To read the previous edition of the VMware Carbon Black Global Incident Response Threat Report, please visit: *COVID-19 Continues to Create a Larger Surface Area for Cyberattacks.*

The results at a glance

82%
of organizations encounter instances of counter IR during IR engagements

55%
of attacks use island hopping during IR engagements

Government (49 percent) and Media and Entertainment (42 percent)

Industries most often targeted by attacks

54%
of targeted victims experience destructive attacks in IR engagements

50%
of attempted attacks leverage customer malware in IR engagements

28%
Responded that biggest challenge to IR in remote work conditions is overworked skilled security/IT staff

62%
of attacks involve attempted lateral movement

37%
of attacks originate in North America

66%
of attacks involve instances of secondary C2 used on a sleep cycle in IR engagements

Social media sites (37 percent) and Google Drive (46 percent)

Used to help facilitate lateral movements for attackers

Ransomware Attacks (55 percent) Attacks increasingly targeting business entities since the start of the pandemic

64%
of IR and cybersecurity professionals believe the election process and related security is more at risk now than it was during the 2016 election

Russia, North Korea and Iran Countries IR and cybersecurity professionals expect to be a source of hacking attempts during the 2020 presidential election

73%
of IR and cybersecurity professionals believe there will be foreign influence on the 2020 presidential election

Strong passwords and multi-factor authentication, securing voting infrastructure and endpoint controls

The security tools IR and cybersecurity professionals believe should be prioritized ahead of the 2020 presidential election

Sources

This report may contain hyperlinks to non-VMware websites that are created and maintained by third parties who are solely responsible for the content on such websites.

1. FBI.gov, "FBI and Secret Service Working Against COVID-19 Threats," April 2020.
2. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "#Protect2020 Strategic Plan," February 2020.
3. Reuters, "Software vendor Tyler Technologies tells U.S. local government clients it was hacked," September 2020.
4. VMware Carbon Black, "COVID-19 Continues to Create a Larger Surface Area for Cyberattacks," August 2020.
5. World Economic Forum, "The Global Risks Report 2020," January 2020.
6. Cybersecurity & Infrastructure Security Agency, "#Protect2020: Countering Foreign Influence," February 2020.
7. The Hill, "European Union police agency warns of increase in cybercrime due to pandemic," October 2020.
8. The Hill, "FBI sees spike in cyber crime reports during coronavirus pandemic," April 2020.
9. WIRED, "Coronavirus Sets the Stage for Hacking Mayhem," March 2020.
10. National Security Agency Central Security Service, "Exim Mail Transfer Agent Actively Exploited by Russian GRU Cyber Actors," May 2020.
11. ZDNet, "Russian hacker group using HTTP status codes to control malware implants," May 2020.
12. Cybersecurity & Infrastructure Security Agency, "Federal Agency Compromised by Malicious Cyber Actor," September 2020.
13. TechTarget, "Maze ransomware 'cartel' expands with new members," August 2020.
14. See #2
15. FBI.gov, "FBI Denver Educates Community About Election Security and Foreign Malign Influence in Advance of the November Election," October 2020.
16. ZDNet, "Ransomware victims are paying out millions a month. One particular version has cost them the most," March 2020.
17. The Wall Street Journal, "Voters Face a Complicated Election as the Pandemic Remakes Voting," September 2020.
18. Cybersecurity & Infrastructure Security Agency, "APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations," October 2020.
19. VMware Carbon Black," Best Practices for Securing Critical Infrastructure for State and Local Governments," January 2020
20. FBI & CISA, "False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections," September 28, 2020.
21. New York Times, "Ransomware Attacks Take On New Urgency Ahead of Vote," September 27, 2020.
22. Mother Jones, "Researchers Assembled over 100 Voting Machines. Hackers Broke Into Every Single One," September 27, 2019.

VMware September 2020 Survey Methodology

VMware Carbon Black conducted an online survey about trends in incident response and election security in September 2020. Eighty-three Incident Response (IR) and cybersecurity professionals from around the world participated. Percentages in certain questions exceed 100 percent because respondents were asked to check all that apply. Due to rounding, percentages used in all questions may not add up to 100 percent.

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.

VMware and Carbon Black are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and other jurisdictions.

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: VMWCB-EB-GIRTR-R9-02 10/20