



Global Incident Response Threat Report

2022



Weathering the storm: As geopolitically motivated cyberattacks and zero-day exploits proliferate, incident responders are fighting back.

Index:

Introduction →

Key findings →

The eye of the storm: Today's threat landscape →

Shifting winds: How attackers
move about a victim's network →

The state of IR today →

Five best practices for organizations and IR teams →

Case study →

Conclusion →

Methodology →



Introduction

For today's incident responders, combating the ceaseless wave of cyberattacks can feel like being adrift at sea during a never-ending storm. VMware's 2022 Global Incident Response Threat Report takes a deep dive into the headwinds faced by defenders and how security teams attempt to stay the course.

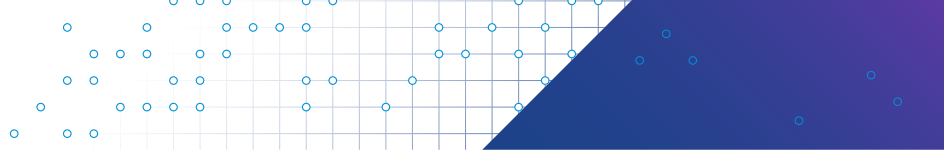
In our annual survey of 125 cybersecurity and incident response (IR) professionals, we found that security teams are still reeling from pandemic disruptions and burnout while bracing for cyberattacks tied to Russia's invasion of Ukraine.

Sixty-five percent of respondents said cyberattacks have increased since Russia invaded Ukraine. In February, for instance, we saw a new type of malware (coined HermeticWiper) deployed in one of the largest targeted attacks in history focused solely on the destruction of critical information and resources.¹ This is part of a growing list of destructive malware deployed against Ukraine, as noted in a joint advisory the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released this spring.²

Zero-day exploits also show no signs of abatement after record levels last year: 62 percent of respondents said they experienced such attacks in the past 12 months, up from 51 percent in 2021.³ This surge can be attributed to geopolitical conflict, too.

"Zero-days are expensive to make—and once they're used, they're not as useful again," says Rick McElroy, principal cybersecurity strategist at VMware. "Nation-states are therefore prime drivers behind the zero-day market, particularly during saber-rattling moments like this."

This year's report delves into a number of other threat areas, including the mounting risks posed by deepfakes, container and cloud vulnerabilities, API security systems, business email compromises (BECs), and extortionary ransomware attacks. The ability of threat actors to move around networks, evade security teams, and leverage these various platforms and attack methods to further penetrate networks and distribute attacks only exacerbates these risks.



Case in point: Once again, the majority of respondents witnessed instances of lateral movement, with 1 in 10 saying they account for at least half of all attacks. And that's just the instances they can see.

"Lateral movement has always been with us," says Karen Worstell, senior cybersecurity strategist at VMware. "What has changed is that an increasing percentage of east-west traffic is not moving through the network. Rather, it stays on the hypervisor as the hypervisor runs more and more workloads. This means that unless system and organization controls are equipped to see the lateral movement between workloads and containers on the hypervisor, security teams are sailing blind in the storm."

This year's report does reveal a bright side: Defenders are successfully implementing new strategies and methods to stem the tide of incursions. For instance, 75 percent of organizations have employed virtual patching as an emergency mechanism, reflecting the growing maturity of security teams.

Nearly 90 percent of respondents now say they are able to disrupt an adversary's activities, and 74 percent report that IR engagements are resolved in a day or less. And while burnout remains a critical issue and a higher number of respondents said they have contemplated leaving their jobs this year than last, overall burnout rates are slightly down from 2021 as organizations take smart steps to address employee wellness.

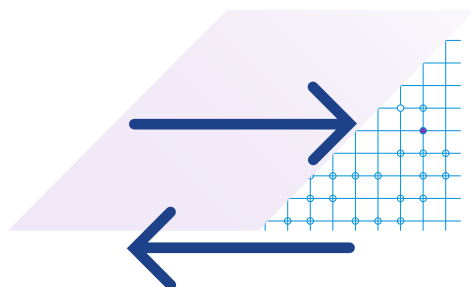
In what follows, we'll cover all this and more to help organizations see and stop more threats while ensuring defenders can weather the storm.

"This means that unless system and organization controls are equipped to see the lateral movement between workloads and containers on the hypervisor, security teams are sailing blind in the storm."

**Karen Worstell,
Senior Cybersecurity
Strategist, VMware**

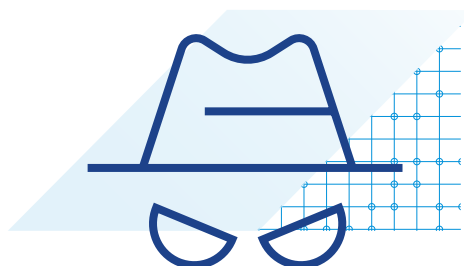


Key findings



Lateral movement is the new battleground.

The majority of respondents witnessed instances of lateral movement in the past year, reporting they appeared in 25 percent of all attacks. Dual-use tools—system tools and legitimate software that can be abused by attackers—leveraged for this purpose went up across the board, with increases of more than 10 percent in the use of script hosts (49 percent) and file storage and synchronization (46 percent) (e.g., Google Drive, OneDrive). This latter finding signals a troubling lack of visibility into cloud storage platforms.



Deepfake attacks shot up 13 percent, with 66 percent of respondents now saying they witnessed them in the past 12 months.

Email was the top delivery method (78 percent) for such attacks, which corresponds with the rise in BECs (i.e., when criminals send messages that appear to come from a known source with a legitimate request). From 2016 to 2021, BEC incidents cost organizations an estimated \$43.3 billion, according to the FBI.⁴



Sixty-five percent of respondents said cyberattacks have increased since Russia invaded Ukraine.

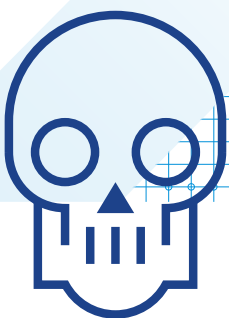
This correlates with findings uncovered in our [Modern Bank Heists report](#), which revealed that a majority of financial leaders said Russia posed the greatest concern to their institution.⁵



Zero-day exploits were encountered by 62 percent of respondents in the past 12 months, an 11 percent increase from last year. These costly, often custom-made exploits continue to skyrocket, in large part due to mounting geopolitical conflict.



Nearly one-quarter of attacks (23 percent) now compromise API security as these platforms emerge as a promising new endpoint for threat actors to exploit. The top types of API attacks include data exposure (encountered by 42 percent of respondents in the past year), SQL and API injection attacks (37 percent and 34 percent, respectively), and distributed denial-of-service attacks (33 percent). These findings suggest attackers are not only seeking to compromise API security as an end in itself but are leveraging it to distribute additional, often destructive attacks, also known as progressive API attacks.



Nearly 60 percent of respondents experienced a ransomware attack in the past 12 months as prominent cyber cartels continue to extort organizations through double extortion techniques, data auctions and blackmail.



IR professionals are fighting back, with 87 percent saying they are able to disrupt a cybercriminal's activities sometimes (50 percent) or very often (37 percent).

They're using new techniques to do so: Three-quarters of respondents (75 percent) say they are now deploying virtual patching as an emergency mechanism.

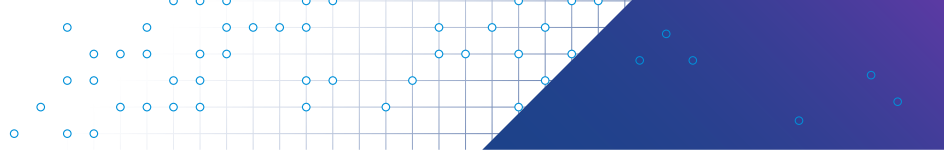


While burnout rates dropped slightly from last year, it remains a critical issue.

Forty-seven percent said they experienced burnout or extreme stress in the past 12 months, down from 51 percent last year, and more than two-thirds of respondents said their workplaces have implemented wellness programs to combat it. Yet unfortunately, 69 percent (compared to 65 percent in 2021) of respondents experiencing these symptoms still considered leaving their job as a result.



The eye of the storm: Today's threat landscape



“Ukraine was not the first ‘cyber war’...but it was the first major conflict involving large-scale cyber operations,” wrote James Andrew Lewis, senior vice president and director at the Center for Strategic and International Studies, in June.⁶

In the months leading up to the invasion, Russian cyberattacks hit Ukraine’s largest gas retailer, their defense ministry’s website, and at least 21 companies—including Chevron, Cheniere Energy and Kinder Morgan—involved in the liquefied natural gas industry, among numerous other targets. That onslaught continued after the invasion started, with new malware and exploits targeting Ukrainian government networks, domestic telecom companies, and other critical infrastructure. Many had downstream effects: For instance, an attack on satellite internet provider Viasat

caused communications outages that ultimately led to the malfunction of nearly 6,000 wind turbines in Germany and “disruptions to thousands of organizations across Europe.”⁷

62 percent of respondents encountered a zero-day exploit in the past 12 months, compared to 51 percent in 2021.

Our report reflects those trends, with 65 percent of respondents noting an increase in cyberattacks since Russia invaded Ukraine. Zero-day exploits, often developed by nation-states and/or cyber cartels with the capital to uncover software vulnerabilities and backdoors, also saw a steep rise, with 62 percent of respondents having encountered one in the past 12 months (compared to 51 percent in 2021).

As for existing exploits, the Log4j vulnerability, found in a popular open source Java logging library, has been leveraged by hackers in more

than 25 million attack attempts in the past six months alone.⁸ Open source development tools are also a susceptible area for zero-day exploits, such as the vulnerability found in a tool used for Kubernetes software.⁹ In keeping with the ongoing surge in zero-day exploits, 71 percent of respondents said an attack uncovered a vulnerability they didn’t even know they had. This means awareness—and visibility—is key.

“Unfortunately, 100 percent prevention of zero-days is nearly impossible,” says Tom Kellermann, head of cybersecurity strategy at VMware. “What defenders can do is implement network and endpoint protection and response tools that scan for vulnerabilities listed in CISA’s Known Exploited Vulnerabilities Catalog, while also ensuring they have visibility throughout their infrastructure.”¹⁰

Malware, ransomware and cyber extortion

Destructive malware—including malware families such as Emotet that were presumed to have been taken down by Western governments—is also seeing a resurgence aligned with recent geopolitical events.¹¹ The FBI and CISA, for instance, released an advisory earlier this year about destructive malware, such as WhisperGate and [HermeticWiper](#), used against organizations in Ukraine to “destroy computer systems and render them inoperable.”¹²

Though survey respondents only saw custom malware in roughly one-third (27 percent) of attacks, those with typical antivirus software might not have the capabilities to detect the behavioral anomalies such malware poses. With that said, U.S. and U.K. respondents witnessed more of these attacks (30 percent and 34 percent, respectively), which makes sense given their early and ongoing support of Ukraine.

The predominance of ransomware attacks, often buttressed by e-crime groups’ collaborations on the dark web, has yet to let up either.



57%

of respondents said they encountered such attacks in the past 12 months.



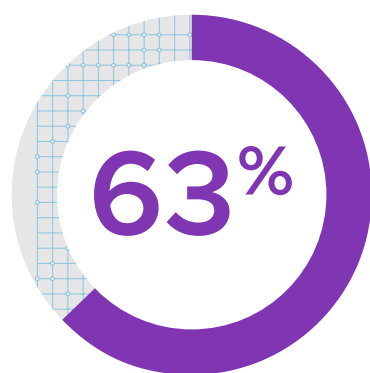
66%

encountered affiliate programs and/or partnerships between ransomware groups.

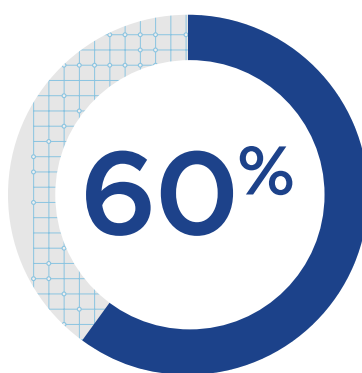
“In the past few years, everything in the criminal markets has become more centralized, with major cartels offering services to affiliate programs,” says McElroy. “This not only heightens risks for organizations but makes attribution extremely tough.”

What’s more, these groups have transformed the traditional aims of ransomware into something even more sinister: cyber extortion. In other words, criminals no longer simply want to get a ransom paid but are staging multilevel campaigns to progressively extort their victims.

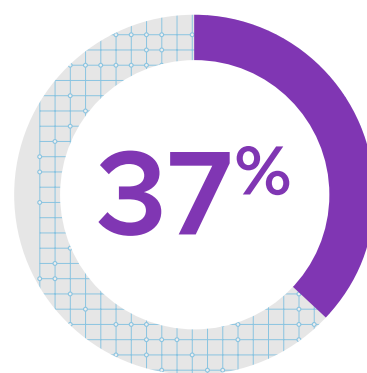
This year’s survey revealed one-quarter of all ransomware attacks included double extortion techniques, with top methods including:



Blackmail



Data auction



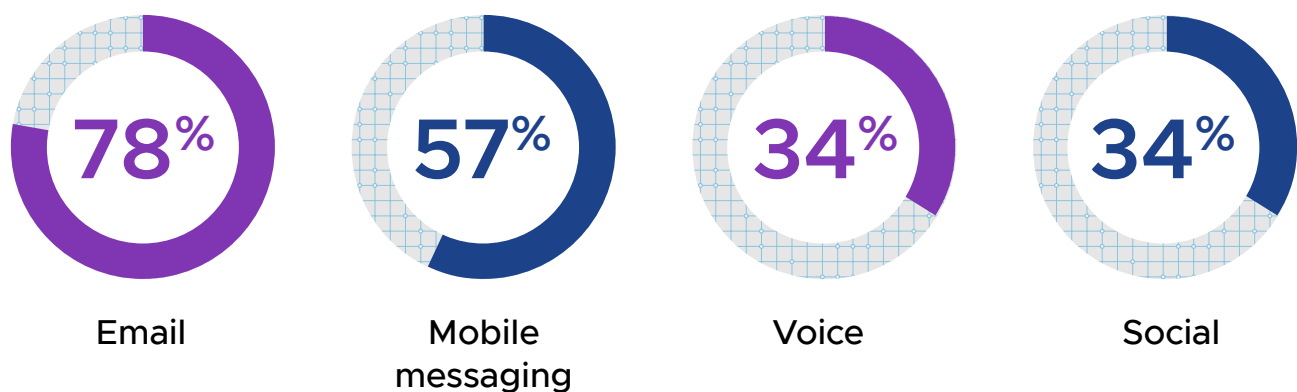
Name and shame

Deepfakes

In March, a video posted to social media appeared to show Ukrainian President Volodymyr Zelenskyy directing his soldiers to surrender to Russian forces.¹³ It wasn’t real, of course—Zelenskyy denounced it as false soon after—but it provides yet another example of the potential threats posed by deepfake technology.

The percentage of respondents who saw malicious deepfakes used as part of an attack went up 13 percent this year to 66 percent. The FBI concurs, having recently cited an increase in complaints involving “the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions.”¹⁴

The majority of respondents said deepfake attacks most often took the form of video (58 percent) rather than audio (42 percent), and top delivery methods included:



New platforms are also increasingly being leveraged for such attacks, including third-party meeting applications (31 percent) and business collaboration tools (27 percent), in the form of business communication compromises (BCCs). Scams were cited as these attacks’ primary purpose (60 percent), while IT (47 percent) was listed as the top target sector, followed by finance (22 percent) and telecom (13 percent).

Worstell says the fact these attacks are going after the IT industry is particularly significant. “The successful SolarWinds attack has provided a formidable blueprint for threat actors looking to target vendors. Targeting IT is only the start of an adversary’s campaign...it’s just a way to get in the door. Attackers know that if they go through IT, they may very well get the keys to the kingdom.”

Attackers looking to infiltrate business email to, for instance, perform an unauthorized transfer of funds can also leverage deepfake technology. There's a reason that business email compromise has been called a "\$43B headache"—following the FBI's report highlighting the costs of such attacks.¹⁵ A hacking demonstration by Rachel Tobac on Jeffrey Katzenberg provides a detailed example of how an attacker can pair deepfake technology with a BEC to manipulate targeted individuals.¹⁶

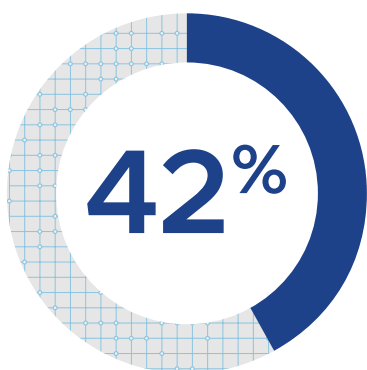
Emerging attack types and vulnerabilities: API security, containers and insider threats

APIs, which allow two software components to communicate with each another, are also increasingly under threat.

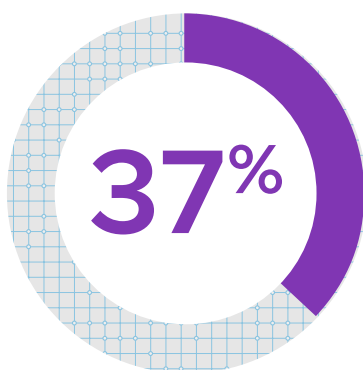


23%

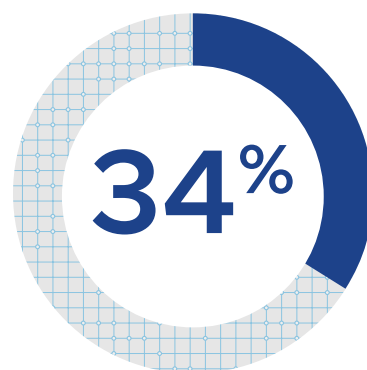
of all attacks seen by respondents in the past 12 months compromised API security, with top API attack types including:



Data exposure attacks



SQL injection attacks



API injection attacks

Worse, once these systems are breached, they can be used to distribute attacks as well, known as progressive API attacks. Organizations should familiarize themselves with the Open Web Application Security Project (OWASP) Top 10 security vulnerabilities and the methodologies used to mitigate them.

“As workloads and applications proliferate, APIs have become the new frontier for attackers,” says Chad Skipper, global security technologist at VMware. “As everything moves to the cloud and apps increasingly talk with one another, it can be difficult to obtain visibility and detect anomalies in APIs.”

Meanwhile, 75 percent of respondents (compared to 64 percent in 2021) said they had encountered exploits of vulnerabilities in another cloud native technology: containers. The growing use of these applications, their ephemeral nature (a container’s average lifetime is five minutes, and development teams constantly spin out new ones), and their use of third-party registries provide more entry points for attackers and underscore the importance of image hardening to help ensure only approved images are deployed in production.¹⁷



Finally, malicious insider attacks—in which an organization’s current or former employee, contractor or business partner uses their access to critical assets to facilitate an attack—are on the rise, according to a World Economic Forum report.¹⁸ Our survey found that 41 percent of respondents encountered attacks involving insiders over the past year, underscoring the increasingly critical nature of talent management when it comes to cybersecurity controls.



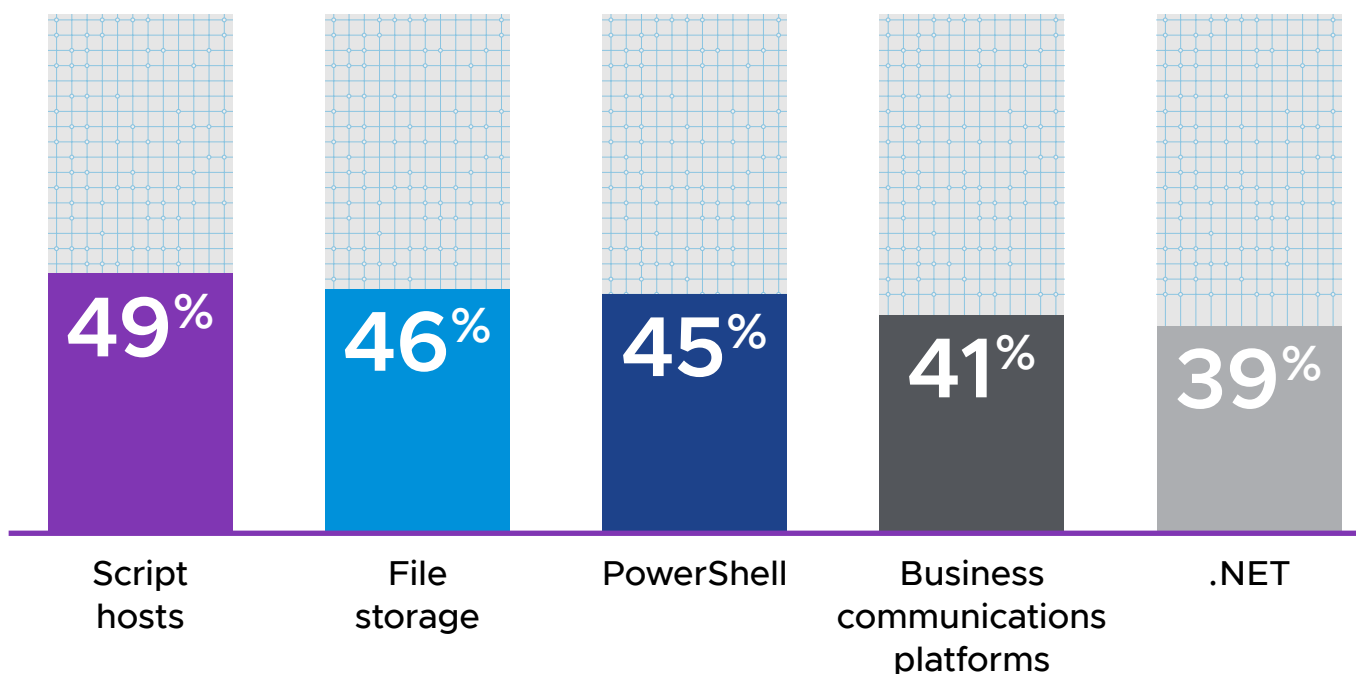
Shifting winds: How attackers move about a victim's network

“CISOs invest most heavily in two areas: technology to protect the perimeter of their networks, and technology to make sure the PCs and other endpoint devices used by employees are not compromised,” [writes](#) Tom Gillis, senior vice president and general manager of VMware’s Networking and Advanced Security Business Group.¹⁹

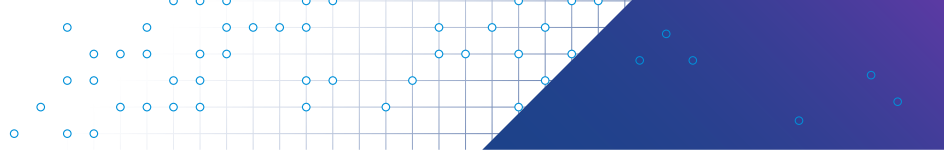
Yet this has done virtually nothing to stop today’s attackers from compromising endpoints, which means defenders should reorient their focus around the applications, data centers, access points and other infrastructure hackers can access once they’ve breached external security barriers.

“In today’s complex networks, there is no such thing as a defensible perimeter,” says Worstell. “Organizations must therefore pivot to a strategy that protects the internal resources and previously trusted services in ways most have yet to do.”

This year’s survey provides sobering insight into the pressing need to provide such a strategy. Lateral movement, for instance, was seen in one-quarter of all attacks, with attackers leveraging:



Attackers also used numerous other dual-purpose tools to rummage around inside networks.



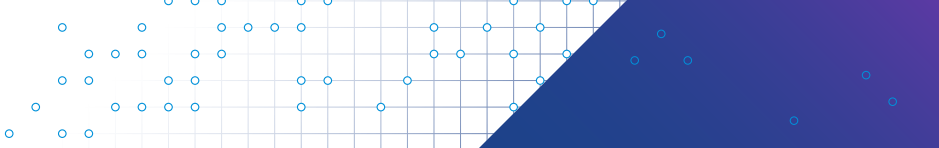
As Gillis observes: “Many of the most sophisticated attackers spend their days devising ways to sneak into the massive flow of data that takes place behind the perimeter. Often, the plan is to obfuscate payloads and hide their malicious activities within legitimate traffic and slip it into this ‘East-West’ traffic, which can be orders of magnitude larger than the relative trickles of ‘North-South’ data that flows past a firewall or onto an endpoint. Once inside, smart attackers bide their time, hiding within the common noise of your network, discovering assets, moving laterally leveraging common ports and protocols waiting for opportunities to do the most damage—say, to launch a ransomware attack or surreptitiously steal customer data.”

An analysis of the telemetry within [VMware Contexa™](#)—full-fidelity cloud-delivered threat intelligence that’s built into VMware security products—offers additional color and nuance to this year’s findings. In April and May 2022 alone, nearly half of intrusions contained a lateral movement event, with most involving the use of remote access tools (RATs) or the use of existing services, such as the Remote Desktop Protocol (RDP) or PsExec.²⁰ Adversaries can leverage RATs to establish staging servers, for example, which can be used to target additional systems with ransomware and monetize access by extorting victim data or stealing resources from cloud services.

For her part, Worstell believes lateral movement might be even more common than our survey data would suggest: “There’s no meaningful attack that doesn’t involve starting in one place and moving to another. More and more attacks are happening within the hypervisor, and many organizations simply don’t have the capabilities to see it.”

Counter IR and evasion tactics

Today’s threat actors possess increasingly sophisticated methods for evading defenders and countering incident response. These techniques—such as resetting passwords (seen by 46 percent of respondents), using trusted software (38 percent), and manipulating time stamps (up to 62 percent from 58 percent last year)—allow attackers to move around inside a network and make it more difficult for IR teams to detect their activities.



Adversaries are also going after IR teams themselves, whether by targeting responders directly (33 percent), tampering with agents (28 percent), or monitoring in-band IR communications (23 percent). The outcome is often destructive, as our latest Modern Bank Heists survey—which reported a 17 percent increase in destructive attacks against financial institutions—revealed earlier this year.²¹

“Mucking with time and tampering with agents are two of the most prominent destructive techniques we’ve seen cybercriminals deploy,” says McElroy. “There needs to be continued innovation around tamper-resistant security tools, while security teams need to practice incident response without the tooling and communication systems they’re used to.”

A VMware Contexta analysis reveals additional evasion types that have been popular within the past six months.²² Evasive tactics implemented via malware include checking disk size, stalling against their analysis environment, detecting the analysis environment by checking the sandbox name, and checking for the presence of keyboard drivers and current memory availability.

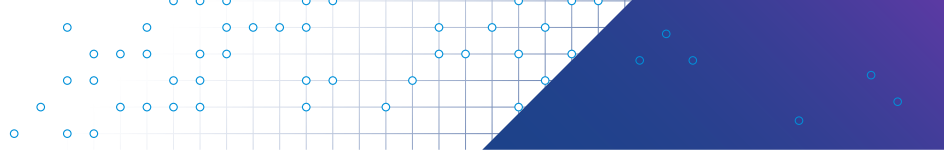
“These techniques aren’t simply used to evade detection,” Skipper said. “They’re also used by adversaries as a means of discovery, to get a sense of whether they’re in an evaluation environment and, if so, abort. For instance, threat actors are checking for the presence of certain keyboard drivers, like Cyrillic; if found on the system they’re trying to compromise, they immediately abort their malicious activity. IR teams therefore need a sandbox that imitates the entire environment—including the CPU, memory and OS—enabling them to see all processes and actions that can help detect and stop these evasions in their tracks.”

“These techniques aren’t simply used to evade detection. They’re also used by adversaries as a means of discovery.”

**Chad Skipper,
Global Security
Technologist, VMware**



The state of IR today



Despite the maelstrom facing today's IR teams, our survey found promising indications that defenders are adapting their responses to effectively fight back.

The vast majority of respondents said they actively disrupt cybercriminals' activities sometimes (50 percent) or very often (37 percent). Most also said cybercriminals are inside the environment only hours (43 percent) or minutes (26 percent) before an investigation occurs, and that engagements are resolved fairly quickly: within a day (23 percent), hours (34 percent), or even minutes (17 percent).

“That [security teams] now have emergency processes in place speaks greatly to the maturity of security programs—not to mention virtual patching is an effective way to disrupt today’s attackers.”

Rick McElroy,
Principal Cybersecurity
Strategist, VMware

They've also adopted new techniques. For instance, 75 percent said their organization or client employed virtual patching as an emergency mechanism.

“Not too long ago, security teams could not get approval for virtual patching,” McElroy says. “That they now have emergency processes in place speaks greatly to the maturity of security programs—not to mention virtual patching is an effective way to disrupt today’s attackers.”

There's ample room for improvement, however, when it comes to visibility into east-west traffic. While the majority of respondents said they have visibility into the cloud (80 percent) and their network (66 percent), that doesn't account for visibility within the cloud or network itself.

Burnout

The great news coming out of this year's report is that companies are paying more attention to relieving workplace stress.

These efforts are having a positive impact on cybersecurity teams. Though still a critical issue—47 percent said they experienced extreme stress or burnout in the past 12 months—that share dropped from 51 percent last year, and more than two-thirds of respondents said their workplaces have implemented wellness programs to combat it. Among these respondents, the programs offered at their organizations include flexible hours (73 percent), investment in further education (45 percent), coaching/therapy (45 percent), well-being days off (40 percent), onsite fitness programs (38 percent), and bonus incentives for successful attack prevention or defense (28 percent).

The most helpful of these programs were:



72%

flexible hours (cited as extremely helpful by respondents whose organizations offered them).



44%

investment in further education (cited as extremely helpful).



45%

coaching/therapy (cited as extremely helpful).

Significantly, those are the top three initiatives that respondents whose workplaces do not offer wellness programs said would help ease burnout.

There's still room for improvement, though. Sixty-nine percent of respondents experiencing extreme stress or burnout said they have considered leaving their job as a result.

“Broadly speaking, companies are taking the right steps when it comes to easing burnout among cybersecurity professionals,” says McElroy. “But solving this issue isn’t a simple, one-time fix. Now is the time to really double down on wellness efforts, such as flexible hours, more education, and coaching and therapy.”

“Now is the time to really double down on wellness efforts, such as flexible hours, more education, and coaching and therapy.”

Rick McElroy,
Principal Cybersecurity
Strategist, VMware



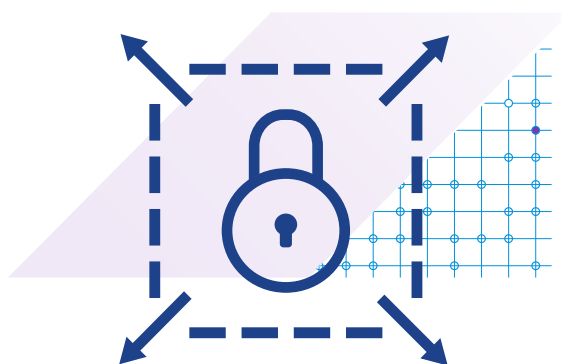


Five best practices for organizations and IR teams

To defend an ever-broadening attack surface, security teams need an adequate level of visibility across workloads, devices, users and networks to detect, protect and respond to cyberthreats.

“Too often, security teams are forced to make decisions with incomplete and inaccurate data,” Skipper says. “This is because they are only sampling parts of the network traffic, not all of it. This lack of visibility and understanding of the network inhibits their ability to implement a granular security strategy, while their efforts to detect and stop lateral movement of attacks are stymied due to the limited context of their systems.”

Here’s how they can improve their defense going forward.



- 1. Focus on workloads holistically.** Many companies focus on keeping compromised applications and devices out of the network. But rather than just looking for anomalous behavior and vulnerabilities at these entry points, companies must understand the inner workings of their entire workload.



2. **Inspect in-band traffic.** Many modern attacks succeed by disguising themselves as legitimate IT practices. For example, by using accepted protocols (such as the LDAP protocol that companies use to store usernames and passwords), attackers may connect to systems that should be off-limits. Don't assume traffic shipped in a familiar wrapper is safe.



3. **Integrate your network detection and response (NDR) with your endpoint detection and response (EDR).** Detection and response technology employs real-time, continuous monitoring of systems to detect and investigate potential threats before using automation to contain and remove them. By bringing together EDR and NDR, enterprises can have access to a broad and deep data set to lay a solid security foundation, and gain visibility into both the endpoint and network—the basis of extended detection and response (XDR).



- 4. Embrace Zero Trust principles.** This broad approach to security assumes every digital transaction could be dangerous and emphasizes strong threat hunting and IR capabilities with broad visibility for the assumption of a breach, as well as robust identity, access and attribute management for every interaction between users and resources and among resources themselves.

In addition to continuous security monitoring, it requires all users to be authenticated and capable of accessing only authorized, relevant systems. This reduces the blast radius of an attack by disabling any east-west spread to other systems. To get started, security teams should familiarize themselves with standards from the National Institute of Standards and Technology (NIST)²³ and The Open Group.²⁴



- 5. Conduct continuous threat hunting.** Security teams should assume attackers have multiple avenues into their organization. Threat hunting on all devices can help security teams detect behavioral anomalies as adversaries can maintain clandestine persistence in an organization's system.



Case study

VMware Carbon Black Cloud Managed Detection and Response™ for endpoints and workloads was introduced in [December 2021](#) to fill the gaps of understaffed security teams and help enterprises respond more quickly to cyberattacks. Since Carbon Black Cloud Managed Detection and Response went live, its threat analysts have seen a variety of attacks attempting to compromise customer environments.

With attackers continuing to leverage PowerShell to facilitate lateral movement, the Carbon Black Cloud Managed Detection and Response team observed a living-off-the-land (LotL) attack within a customer's environment that abused mshta.exe (a known Windows application) to execute a fileless PowerShell script that communicated over the network to a command and control (C2) server. After conducting a historical analysis within the customer's environment, the team was able to link the attack to a policy misconfiguration by the customer's administrator that allowed the device to be infected months prior and enabled threat actors to gain access to the environment. When the activity was initially observed by the customer's internal security team, it was reported as normal and expected behavior. Their lack of information and resources to associate the indicators of compromise (IOCs) with its attributed attack profile ultimately let the device communicate with the C2 server sporadically over at least a two-month time frame, as well as successfully infect additional devices on their network.



Analysts mitigate threats according to the severity of the threat and the operational impact of the asset it was discovered on. Mitigation options include hash banning, reconfiguring policy rules, reassigning asset policies, and quarantining the asset from the network. For this incident, the analyst determined that cloning the device's assigned policy and drafting custom blocking rules tailored according to the observed behavior would be sufficient to contain the threat with limited disruption to business operations. The infected device was also quarantined from the internal network to stop the spread to additional devices. It's important to note that due to the sensitive nature of allowing a third party to manipulate assets within your

network, it was a purposeful decision that these additional actions require customer opt-in through policy configuration to ensure the customer maintains control and expectations as to what can be modified within their own network. In less than two hours, the impacted devices were quarantined and awaiting remediation, the customer was notified, and the environment was scanned for further IOCs. Ultimately, it was determined the IOCs for this incident resembled those attributed to the DarkSide ransomware campaign, which is a financially motivated threat group that targets high-value organizations for ransom.

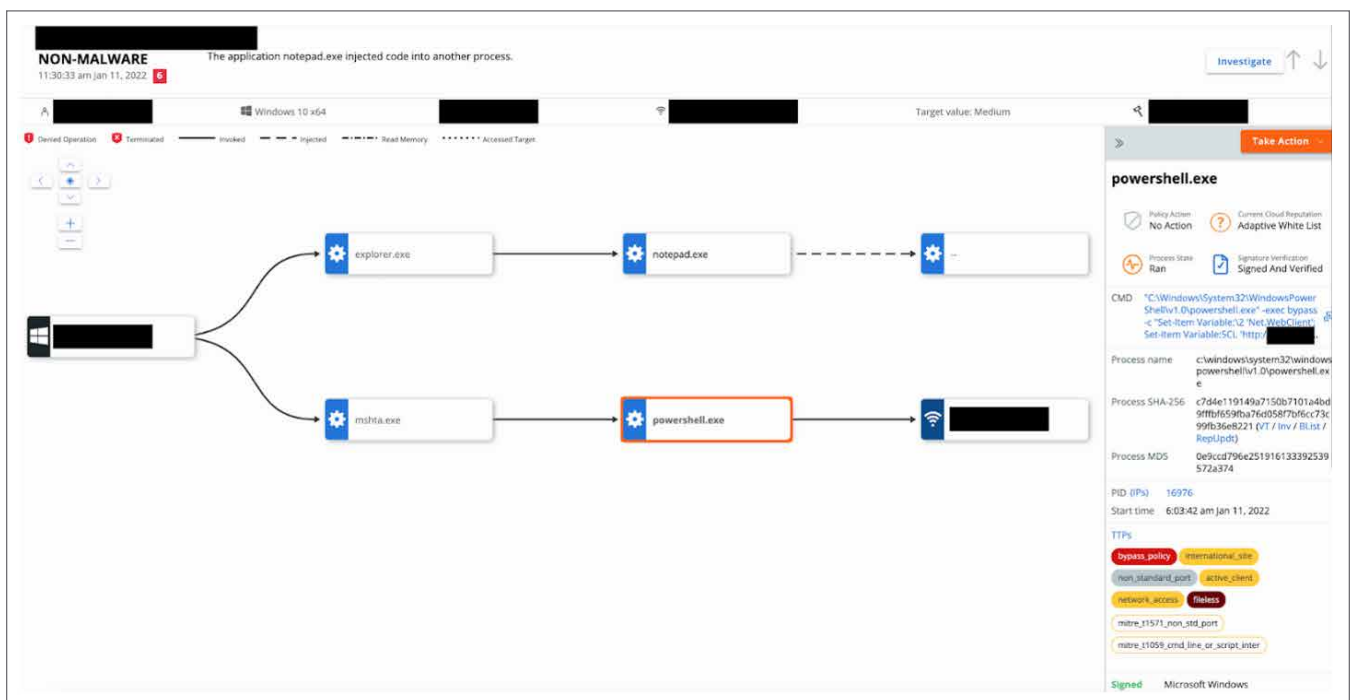


Figure 1: Attacker leveraging mshta.exe and PowerShell to communicate with the C2 server.

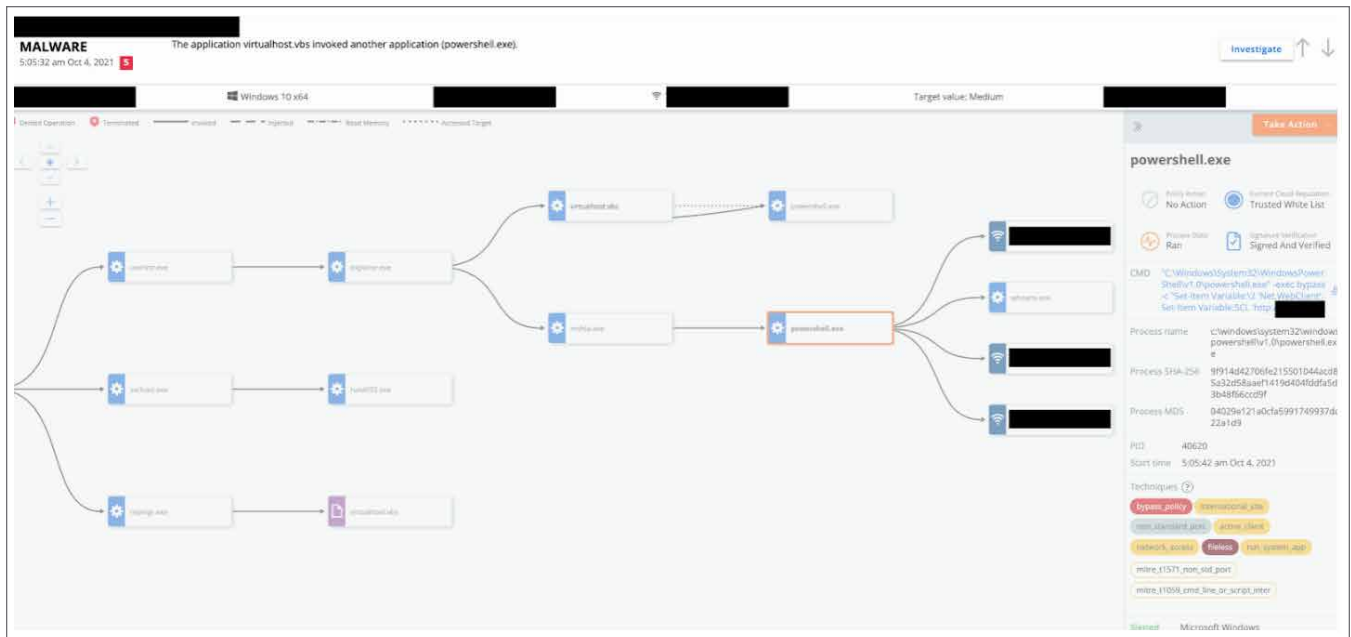


Figure 2: External C2 communication from the infected device.

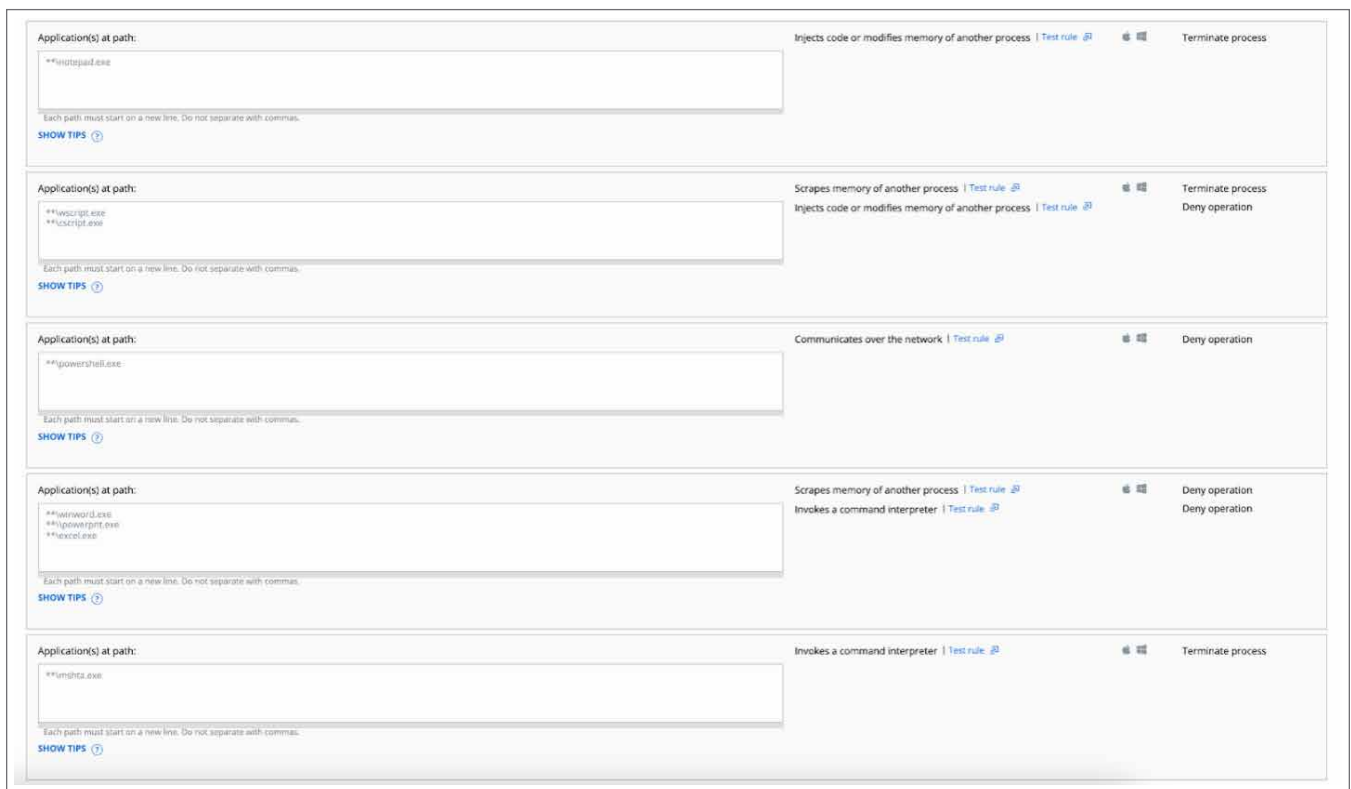
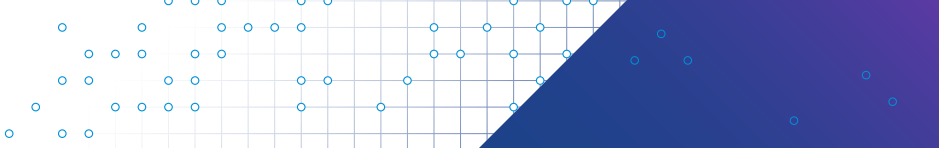


Figure 3: Drafted policy changes to contain the observed threat.



Conclusion



The past two years have placed a heavy burden on IR teams. Unfortunately, the war in Ukraine is ratcheting up the pressure yet again just as cybersecurity professionals began to acclimate to pandemic-related disruptions.

“The maturity of the geopolitical attacks we’ve seen continues to grow, as nation-states and cartels are joining forces to create new and destructive zero-day exploits,” says Kellermann. “Meanwhile, malware families that were presumed to have been taken down have proven their resiliency, ransomware has become cyber extortion, and new endpoints—such as APIs and containers—are increasingly vulnerable.”

Despite this turbulent threat landscape, numerous positives have emerged from the recent tumult. More and more government agencies have engaged in information sharing to help defenders get out ahead of attacks, while security professionals have adopted new detection, protection and response techniques to disrupt cybercriminals’ activities sooner. In every case, the more visibility they have across today’s widening attack surface, the better equipped they’ll be to defeat their adversaries.

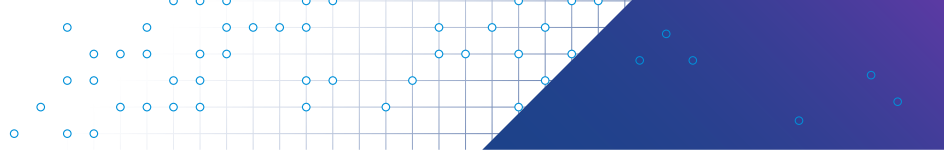
Though the waters ahead will certainly be choppy, defenders have proven that if they continually learn and adapt to new conditions, they can successfully weather the storm.

“The maturity of the geopolitical attacks we’ve seen continues to grow, as nation-states and cartels are joining forces to create new and destructive zero-day exploits.”

**Tom Kellermann,
Head of Cybersecurity
Strategy, VMware**

Methodology

VMware conducted an online survey about trends in the incident response landscape in June 2022, and 125 cybersecurity and incident response 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 in all questions may not add up to 100 percent. To read last year’s report, please visit [Global Incident Response Threat Report: Manipulating Reality](#).



Sources

1. VMware. “Hermetic Malware: Multi-component Threat Targeting Ukraine Organizations.” March 4, 2022.
2. CISA and the FBI. “Update: Destructive Malware Targeting Organizations in Ukraine.” April 28, 2022.
3. VMware. “Global Incident Response Threat Report: Manipulating Reality.” August 2, 2021.
4. FBI. “Business Email Compromise: The \$43 Billion Scam.” May 4, 2022.
5. VMware. “Modern Bank Heists 5.0: The Escalation from Dwell to Destruction.” April 20, 2022.
6. Center for Strategic and International Studies. “Cyber War and Ukraine.” James Andrew Lewis. June 16, 2022.
7. Center for Strategic and International Studies. “The Hidden War in Ukraine.” Emily Harding. June 15, 2022.
8. VMware Contexta Analysis. June 2022.
9. Venture Beat. “Major vulnerability found in open source dev tool for Kubernetes.” Kyle Alspach. February 3, 2022.
10. CISA. “Known Exploited Vulnerabilities Catalog.”
11. VMware. “Emotet Is Not Dead (Yet).” January 21, 2022.
12. CISA and the FBI. “Update: Destructive Malware Targeting Organizations in Ukraine.” April 28, 2022.
13. Congressional Research Service. “Deep Fakes and National Security.” June 3, 2022.
14. FBI. “Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions.” June 28, 2022.
15. Threatpost. “FBI: Rise in Business Email-based Attacks is a \$43B Headache.” Sagar Tiwari. May 9, 2022.
16. Aura. “It Was Easy to Hack a Billionaire.” March 12, 2022.
17. VMware. “Why Vulnerability Management is Key to Your Container Security Strategy.” April 13, 2022.
18. World Economic Forum. “What you need to know about cybersecurity in 2022.” January 18, 2022.
19. VMware. “Why CISOs Should Invest More Inside Their Infrastructure.” Tom Gillis. June 2, 2022.
20. VMware. “Lateral Movement in the Real World: A Quantitative Analysis.” June 29, 2022.
21. VMware. “Modern Bank Heists 5.0: The Escalation from Dwell to Destruction.” April 20, 2022.
22. VMware Contexta Analysis. June 2022.
23. NIST. “Zero Trust Architecture.” August 2020.
24. The Open Group. “Zero Trust Core Principles.” April 2021.



Glossary

API attacks – Hostile usage, or attempted hostile usage, of an API.

Business communication compromise (BCC) – A tactic in which an attacker obtains administrative access to a business communication application account and impersonates the owner's identity to attack the company and its employees, customers or partners.

Business email compromise (BEC) – A tactic in which an attacker obtains access to a business email account and imitates the owner's identity to attack the company and its employees, customers or partners.

Deepfake – Synthetic media (audio or video) that is either wholly created or altered by AI or machine learning to convincingly misrepresent someone as doing or saying something that was not actually done or said.

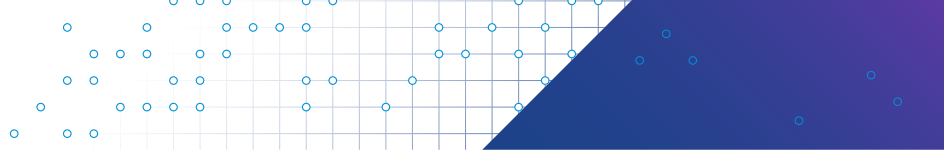
Destructive attack – An attack launched with the goal of destroying data.

Hypervisor – Software that creates and runs virtual machines (VMs).

Lateral movement – A tactic in which an attacker compromises or gains control of one asset within a network and then moves on from that device to others within the same network.

Virtual patching – A security policy enforcement layer that prevents the exploitation of a known vulnerability.

Zero day – A security flaw that has not yet been patched by the vendor and can be exploited by attackers.



About VMware

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control. As the trusted foundation to accelerate innovation, VMware software gives businesses the flexibility and choice they need to build the future. Headquartered in Palo Alto, California, VMware is committed to building a better future through the company's 2030 Agenda. For more information, please visit vmware.com/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com
Copyright © 2022 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 1511973aq-glbl-ir-threat-rprt-2022-uslet 7/22