vmware®

Global Incident Response Threat Report

Manipulating reality: The rise of business communication compromise, time-stamp manipulation, and cloud-jacking empowers adversaries to execute integrity attacks

□ Email me a summary of query results

Queries run against all endpoints by default. However, you can select a specific policy or endpoints.

COMPLIANCE

BitLocker Configuration Details

Description: Bitlocker is a Windows features that encrypts your volume drive.

Results: Details on the BitLocker status for target systems, such as device ID, conversion status, and encryption method.

HYGIENE

Blank Passwords Enabled

Description: Checks for the value of the 'LimitBlankPasswordUse' registry key. The value of the key should be 1, which prevents network connections from accessing the endpo
httpps://www.stigviewer.com/stig/windows_10/2019-01-04/finding/V-63617

Results: Returns "Blank Password Auth via Network Possible" or "Blank Password Auth via Network Not Possible". If "possible" is returned, change the 'LimitBlankPasswor

VULNERABILITY MANAGEMENT

Chrome Extensions

Description: Discover Google Chrome extensions for all users on a target system.. Learn more: https://atttach.mitre.org/techniques/T1176

Results: Lists extension information such as UID, version, locale, and other data.

Introduction

Broadened attack surface, weaponization of new technologies, and industrialization of e-crime continue to shape the modern threat landscape and the ways defenders must fight back, according to the latest VMware Global Incident Response Threat Report.

Management Summary:

Foreword →

Key findings →

The rise of integrity and destructive attacks sows chaos →

Cloud-jacking and lateral movement facilitate destructive attacks →

Industrialization of cybercrime fuels malicious ransomware attacks →

New defender behaviors and the need to practice cyber vigilance →

How to practice cyber vigilance →

The state of incident response in 2021 →

Preparing for the post-pandemic threat landscape →

Foreword

Tom Kellermann, head of cybersecurity strategy, VMware

Rick McElroy, principal cybersecurity strategist, VMware

In 1963, when *The Twilight Zone* aired, the idea that we would eventually get to a place where adversaries could manipulate time, data, audio, and video to wreak havoc—as evinced in certain episodes of the series—was of course seen as far-flung science fiction.

But today, it's become increasingly evident that we are living in a sort of twilight zone, where the goal of modern attackers is to deliver integrity and destructive attacks that distort digital reality, be it via business communication compromise (BCC), the manipulation of time and/or data, or deepfakes. Worse, doing so to colonize one victim's infrastructure is now often just the beginning; the next step is to use that infrastructure (e.g., a cloud network) to launch attacks on others.

“The first adopters of new technologies, like artificial intelligence and machine learning, are always those on the dark web and in nation-states’ intelligence communities,” says Tom Kellermann, head of cybersecurity strategy at VMware. “Today, we’re seeing a nexus between nation-states and cybercriminals—combined with the broadening of the attack surface as a result of COVID-19—continue to rapidly advance the development of increasingly sophisticated and destructive cyberattacks. The digital and physical worlds have converged, and everything can be manipulated by modern-day attackers.”

In our online survey of 123 cybersecurity and incident response (IR) professionals (held between May and June 2021), we gathered insights that offer an in-depth look into this new threat landscape. This includes zero-day attacks that exploit network vulnerabilities, such as the recent attack on Kaseya VSA, a remote monitoring and management tool, which resulted in a $70 million ransom demand from the notorious Russian REvil gang.[1] Other threats abound, including:

- Ransomware attacks, such as the one on Colonial Pipeline, often in partnership with powerful e-crime groups that provide ransomware as a service (RaaS) sold on the dark web
- The rise of cloud-jacking and the use of cloud environments to island hop along a target’s supply chain, as was the case with the SolarWinds breach
- The infiltration of Kubernetes environments
- The frequent deployment of custom malware
- A surge of integrity and destructive attacks achieved; for example, through Chronos attacks, where adversaries manipulate time stamps

It should come as no surprise that defenders, despite their best efforts, are struggling to counter these complex attacks and gain visibility into new environments, such as the cloud, containers, and business communication applications—technologies quickly ushered in by the pandemic. Constantly on alert, defenders are also grappling with blows to their well-being, which carries significant implications for the industry: Of the 51 percent of respondents who experienced extreme stress or burnout during the past 12 months, 65 percent said they have considered leaving their job because of it.

“Burnout is a huge issue with incident response teams, who are handling a spike in engagements in what is still a largely remote environment,” says Rick McElroy, principal cybersecurity strategist at VMware. “It only further underscores the need for leaders to build resilient teams, whether that means considering rotations of work, empowering individuals to take mental health days, or any number of other initiatives aimed at nurturing personal growth and development.”

To combat today’s adversaries, most respondents (81 percent) are also willing to leverage active defense techniques, a spectrum of activity that ranges from deception technology to hacking back. Whereas techniques such as deploying deception grids and microsharding data are useful, hacking back should not be enacted. Security teams must practice cyber vigilance, Kellermann says.

In this report, we’ll outline how to build these resilient, cyber-vigilant IR teams, while also taking a deeper look at the increasingly sophisticated threats facing organizations today. To do so, we’ll draw on the findings gathered from our online survey.

Key findings

Attacks are becoming more destructive and targeted through advanced techniques.

Respondents indicate that targeted **victims now experience integrity and destructive attacks more than 50 percent of the time**. Cybercriminals are achieving this through emerging techniques, such as the **manipulation of time stamps, or Chronos attacks, which nearly 60 percent of respondents have observed**.

With cloud-jacking on the rise, cloud security remains a top priority.

Following the rush to cloud technology amid the pandemic, cybercriminals have continued to exploit these environments to deliver integrity and destructive attacks. **Nearly half (43 percent) of respondents said more than one-third of attacks were targeted at cloud workloads**, with almost one-quarter (22 percent) saying more than half were. Increasingly, attackers are using the cloud to island hop along the victim's supply chain: **49 percent of all attacks targeted the victim via island hopping**. This is compared to the 53 percent of all attacks our respondents witnessed that target the victim directly.

BCC is fast becoming the new business email compromise (BEC).

Catalyzed by the shift to a remote-work environment during COVID-19, adversaries are increasingly leveraging business communication platforms (e.g., Microsoft Teams, Skype, Slack, Google Chat) to move around a given environment and launch sophisticated attacks. When asked which dual-purpose tools are facilitating lateral movement (or living off the land), 32 percent of respondents chose such platforms, trailing only PowerShell and Microsoft's .NET.

The nexus between nation-states and e-crime continues to heighten the threat landscape and exploit vulnerabilities.

Among those who encountered ransomware attacks in the past year, **64 percent witnessed affiliate programs and/or partnerships between ransomware groups**—groups harbored by nation-states such as Russia.[2] The unprecedented collaboration of cybercriminals is being used to exploit vulnerabilities more effectively than ever before (e.g., zero-day attacks), often through the use of **custom malware, which was observed by respondents in more than half (52 percent) of attempted attacks.**

Half (51 percent) of defenders experienced symptoms of extreme stress or burnout,

with 65 percent of respondents saying they've considered leaving their job because of it. Defenders are also looking for new ways to fight back: 81 percent said they are willing to leverage active defense in the next 12 months.

The rise of integrity and destructive attacks sows chaos

Maybe the attacker uses wipers so victims can't recover encrypted data. Or they deploy fake ransomware with no key. Or they get access to your network's Active Directory and start changing payroll information. Or use customized malware to conduct a disruptive denial-of-service attack.

In these and other cases, cybercriminals are ratcheting up their maliciousness. They don't just want to steal from your organization, they want to fundamentally debilitate it in the process.

51%

According to respondents, targeted victims now experience integrity and destructive attacks 51 percent of the time.

80%

Nearly one-third say they see such attacks more than 80 percent of the time.

These have immense consequences: A new report, for instance, argues that the cost of a major cyberattack on a critical U.S. service provider or utility could cost as much if not more than a natural disaster.[3]

One area that's especially vulnerable is industrial control systems (ICS).

"As geopolitical tensions intensify, it could lead to destructive attacks against ICS environments in the manufacturing, transportation, and energy sectors that will escalate as we saw with the Colonial Pipeline attack," Kellermann says. "In turn, new, destructive malware specific to ICS infrastructure will become a hot commodity on the dark web."

Other malware will continue to be customized to the specific target's environment: respondents note that 52 percent of attempted attacks now involve custom malware, compared to 55 percent involving commodity malware. Fifty-three percent of all attacks also now target the victim directly. In other words, this new wave of attacks stems from extensive reconnaissance of the victim. Forty-three percent of respondents say the average duration of such reconnaissance is one to four weeks, while 26 percent say it's more than month, highlighting the need for defenders to assume there is already a breach to uncover.

Another way adversaries can wreak destruction and attack the integrity of targeted individuals, organizations, and systems is through the use of Chronos attacks, or the manipulation of time stamps. Nearly 60 percent of respondents observed adversaries doing just that.

"By manipulating time stamps, attackers can cause a whole lot of damage: They can disrupt entire network operations by changing the times of routers and switches, they can interrupt a defender trying to threat hunt, they can even take advantage of microtransactions before a stock dips and potentially alter the value of capital or trades," McElroy says.

It tracks that in the latest Modern Bank Heists Report from VMware, 41 percent of financial institutions observed the manipulation of time stamps.[4]

Deepfakes are another example. With a "drastic uptick in deepfake technology and service offerings across the dark web"[5] now available, experts are anticipating a surge in the use of such technology in cyberattacks, be it for phishing attempts, BEC, or through BCC via platforms such as Microsoft Teams. In March 2021, the FBI released a report with a headline declaring, "Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations."[6]

"Business communication platforms are the perfect delivery mechanism for deepfakes, because organizations and users implicitly trust them and they operate throughout a given environment," says McElroy. "At the same time, crypto-mining technology, which draws on computing power from across a network, can easily be repurposed by cybercriminals to generate malicious deepfakes. These deepfakes can be hard to detect, and executives should have an out-of-bounds communications channel to verify the integrity of a message before they trust it."

Cloud-jacking and lateral movement facilitate destructive attacks

The rapid and widespread adoption of the cloud offers new opportunities for attackers to conduct sophisticated integrity and destructive attacks.

34%

According to our respondents, one-third of all attacks in the past 12 months leveraged cloud computing. A similar percentage (34 percent) were aimed at cloud workloads.

49%

The imminent concern, according to Kellermann, is that cloud-jacking becomes the future of island hopping. This past year, island hopping was seen in 49 percent of all attacks, and the number might actually be higher than reported given the use of home networks for such attacks.

> "If 2020 was the year of island hopping, where cybercriminals infiltrate large company networks by targeting third parties with lower levels of protection, then we should expect cloud-jacking through public clouds to go mainstream in 2021, particularly with the mass migrations to public clouds to support distributed workforces," Kellermann says.

"If 2020 was the year of island hopping, where cybercriminals infiltrate large company networks by targeting third parties with lower levels of protection, then we should expect cloud-jacking through public clouds to go mainstream in 2021, particularly with the mass migrations to public clouds to support distributed workforces," Kellermann says. "Regrettably, we should expect a public cloud to be commandeered to launch a systemic ransomware attack this fall."

Though 98 percent of CISOs say they already use or plan to shift to a cloud-first security strategy—and despite cloud security being the new security platform most implemented by organizations this past year—vulnerabilities persist.[7]

> "There's a lot of lip service paid to cloud security, but less actual deployment of cloud security controls," says Vigna.

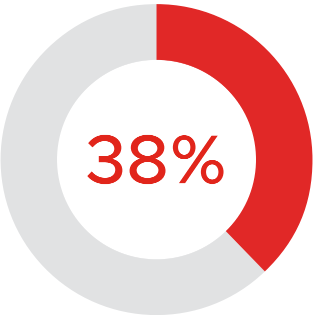
"There's a lot of lip service paid to cloud security, but less actual deployment of cloud security controls," says Giovanni Vigna, senior director of threat intelligence at VMware. "Most of the time, organizations simply turn on features, but that often doesn't strike at the root of the problem. What they need to realize is that the code written to deploy cloud workloads can have as many vulnerabilities as the service it's deploying."

Another emerging vulnerability comes from Kubernetes environments: 64 percent of respondents encountered container images that allow bad actors to exploit vulnerabilities in such environments. Like clouds, Kubernetes can provide a false sense of security.

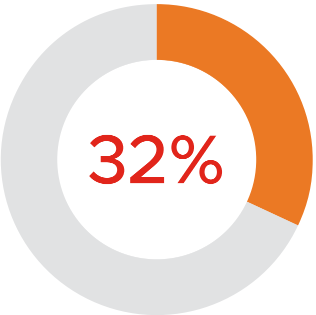
"One way to look at these deployments is as a group of workloads that work together to provide a service; there are many components, but they only have one well-defined user interface that pushes to the outside," adds Vigna. "Because there's only that one endpoint, it gives the perception that there can't be a lot of problems in the environment. But that's a misnomer. It only takes one wrong line of code in one of these workloads to expose vulnerabilities to attackers."

In fact, on July 1, 2021, the National Security Agency (NSA) and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a rare joint alert that warned of widespread brute-force attacks on U.S. and global organizations by Russia's GRU military intelligence agency. These attacks employed Kubernetes software containers to perform the attacks at scale.[8]

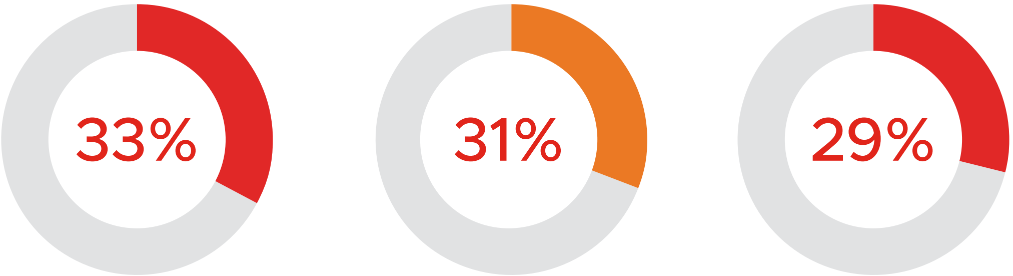
New technologies and platforms are also catalyzing new ways for attackers to move around a given environment—cloud to cloud, system to system, platform to platform—and colonize infrastructures that can allow them to launch attacks onto others.



When survey respondents were asked which dual-purpose tools are facilitating such lateral movement, .NET, a new open source development platform created by Microsoft, surfaced as the second highest response (38 percent), trailing only PowerShell.



Business communication platforms (Microsoft Teams, Skype, Slack, Google Chat), which rose to prominence during COVID-19, were a top choice as well (32 percent).



Other tools facilitating lateral movement included script hosts (where attackers run command line and script-based attacks from within the environment) (33 percent), social media sites (31 percent), and Windows Management Instrumentation (WMI) (29 percent).

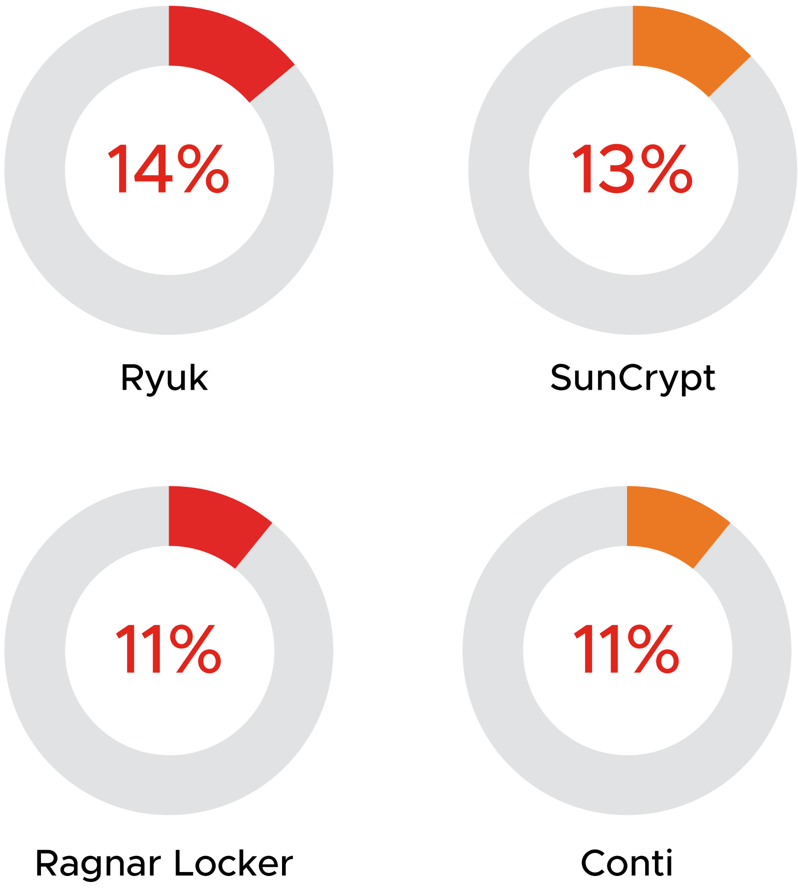
Overall, 61 percent of respondents witnessed attempted lateral movement during the past 12 months.

“Lateral movement has modernized, allowing attackers to launch systemic destructive attacks as evidenced by the attack on Kaseya and its customers,” Kellermann says. “Business communication platforms also pose real risks when it comes to facilitating lateral movement. Defenders have limited visibility, and traditional network security is inadequate to prevent adversaries from infiltrating them.”

Industrialization of cybercrime fuels malicious ransomware attacks

More than 60 percent of respondents encountered ransomware attacks during the past 12 months, and these attacks are becoming increasingly malevolent. This escalation stems from adversaries implementing multistage campaigns involving penetration, persistence, data theft, and extortion. **More than half (52 percent) of ransomware encounters, for instance, included double-extortion techniques**.

The ransomware families most observed include:



“Ryuk has been known to be deployed as part of ongoing geopolitical tensions, such as in attacks against hospitals’ critical infrastructures this past fall during COVID-19,” McElroy says.

These tensions continue to play out in cyberspace, especially given the growing industrialization of e-crime groups under the protection and support of rogue nation-states. “This protection racket has emboldened the cybercrime cartels, as they are seen as national assets, often with untouchable status from Western law enforcement,” says Kellermann. The recent disclosure of the U.S. Secret Service Most Wanted List highlights some of these dark web demigods.[9]

Sixty-four percent of respondents who encountered ransomware also encountered affiliate programs and/or partnerships between such groups. The continued rise of e-crime is now estimated to cost the world $6 trillion in 2021, costs that experts expect to double by 2025.[10]

"The pandemic not only broadened the attack surface but provided the time, capital, and opportunity for cybercrime to industrialize," says Kellermann. "These groups are collaborating on the dark web to form pseudo-legitimate businesses that sell network access points and RaaS, and create affiliate programs to reward partners for assisting in malware delivery. The activity of these groups heightens the need for proactive threat hunting and continuous monitoring to limit exposure and mitigate vulnerabilities."

> "The pandemic not only broadened the attack surface but provided the time, capital, and opportunity for cybercrime to industrialize," says Kellermann.

Then there are the dollar amounts:

↗ $300K

On average, our respondents told us that ransomware attackers demand about $300,000.

↘ $240K

Organizations pay about $240,000.

But there are important distinctions:

↗ $750K

Nearly 20 percent of attackers asked for more than $750,000 in ransom.

↘ $500K

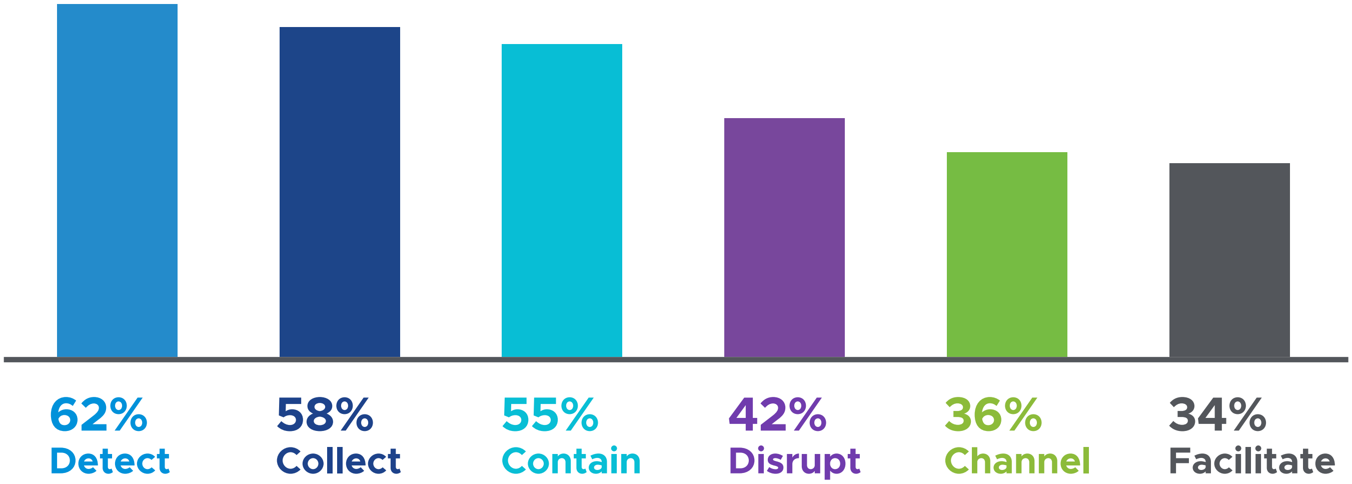
Only 6 percent of organizations paid ransoms of that size or more. The vast majority paid ransoms less than $500,000, and 21 percent said they did not pay at all.

This is important context as movement on Capitol Hill points to a potential ban on ransomware payments,[11] and with Deputy Attorney General Lisa Monaco elevating ransomware attacks to the same threat level as terrorist attacks.[12] Even more recently, NATO amended Article 5 to say any destructive cyberattack against critical infrastructures would be considered an attack on all NATO members.[13]

New defender behaviors and the need to practice cyber vigilance

In the face of this new threat landscape, defenders are ready to go to new lengths to fight back. **Eighty-one percent of respondents said they would be willing to leverage active defense in the next 12 months**, involving tactics such as:

- Detect – Establish or maintain awareness into what an adversary is doing
- Collect – Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity
- Contain – Prevent an adversary from moving outside specific bounds or constraints
- Disrupt – Prevent an adversary from conducting part or all of their mission[14]



"Companies rightly feel like they should be able to defend themselves," McElroy says. "But that could go wrong if organizations start to conduct escalation of force with no clear rules and no expertise in offensive security."

Those methods may involve, for instance, certain elements of Channel (guide an adversary down a specific path or in a specific direction) or Facilitate (enable an adversary to conduct part or all of their mission).

How to practice cyber vigilance

To combat today's attackers, we recommend practicing cyber vigilance. Here are some best practices to get started.

Increase situational awareness. It is critical that organizations take a proactive and comprehensive approach to security, regardless of sector or size. Telemetry is fundamental in achieving this situational awareness and is most effective when the organization's network detection and response platform is integrated with its endpoint protection platform.

Expand cloud security. Migration to the cloud (and cloud-jacking) shows no sign of slowing down, which must result in security that extends across workloads, containers, and Kubernetes environments.

Track identities on the move. Today's attacks do not have a distinct beginning or end. Instead, adversaries conduct reconnaissance to learn as much as they can about organizations and often move covertly throughout a target's network. To ensure adequate protection, security teams need the ability to accurately track identities as they move. That means:

- Implementing just-in-time administration and multifactor authentication on all external assets
- Leveraging a single sign-on (SSO) provider to allow for centralized and seamless authentication across the vastly distributed work environment
- Applying the principle of least privilege

Operationalize hardening and patching. With attackers continuing to exploit vulnerabilities, it's critical to leverage industry best practices for hardening and patching. Ensure IT operations and security are on the same page with vulnerability data. Maintain agreed-on service-level agreements (SLAs) for patching.

Apply micro-segmentation. Limit an adversary's ability to move laterally within the organization. For instance, forcing intruders to cross trust boundaries provides better opportunities for detection and prevention.

Activate your threat hunting program. Prepare for the worst, hope for the best. 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. Threat hunting should be conducted on a weekly basis.

The state of incident response in 2021

In the first half of 2021 alone, 62 percent of respondents said their IR team had more than 11 threat response engagements, and 30 percent of those reported their teams had more than 21. This represents an extension of the spike in attacks witnessed in 2020: In the latest VMware Global Security Insights Report, three-quarters (76 percent) of the 3,542 respondents said the number of attacks they faced increased in the past year.[15]

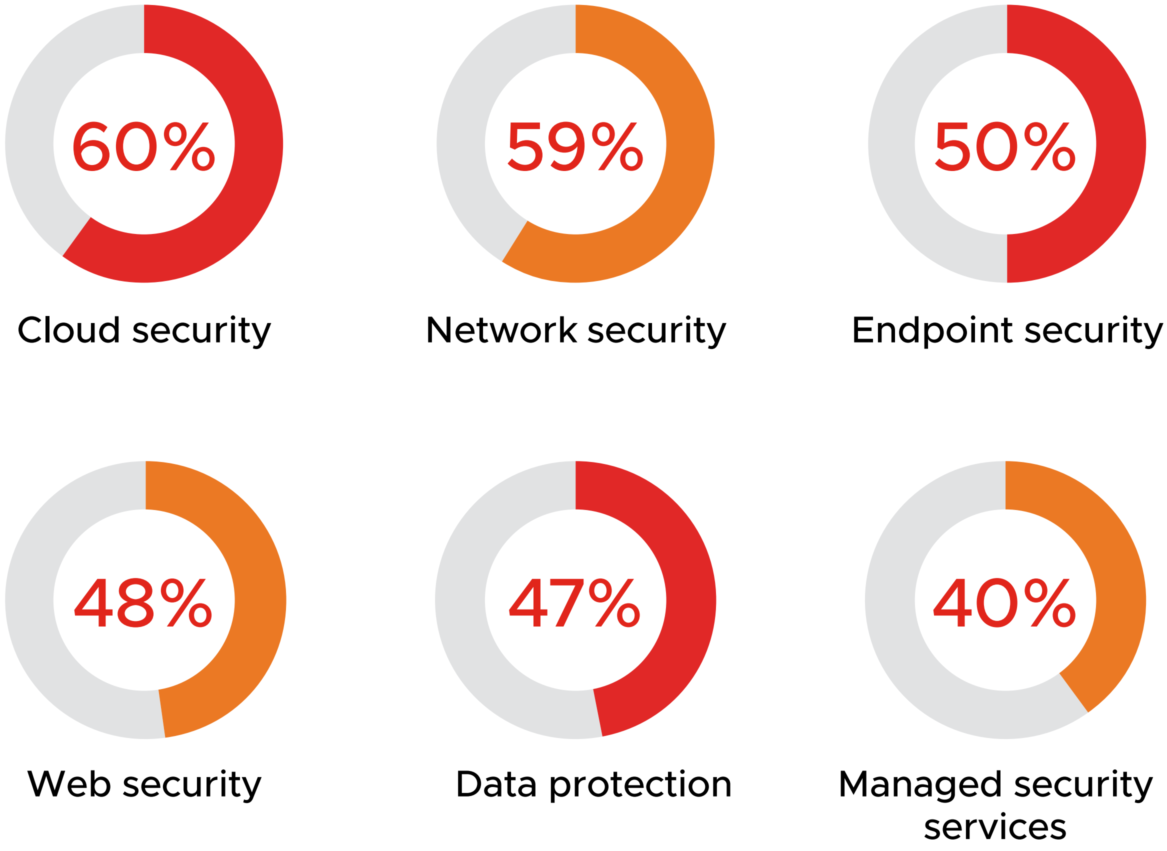
Additionally concerning, our survey shows that nearly one-third (28 percent) of IR engagements in 2020 and H1 2021 involved repeat customers/client organizations.

“This speaks in large part to the renaissance of rootkits, which are included as a component of today’s ransomware attacks,” Kellermann says. “Defenders must heighten their vigilance for these techniques, particularly when it comes to C2 on a sleep cycle.”

The good news? With better telemetry and the adoption of the MITRE D3fense™ framework, IR teams are moving faster. Twenty-eight percent of respondents said the time spent on each IR engagement took just hours in H1 2021, compared with only 18 percent in 2018. And just 17 percent of respondents said they spent more than a month in H1 2021, compared to nearly 30 percent who said as much for 2018 engagements.

> “Being in cybersecurity is like being an air traffic controller; you’re constantly watching the radar and have to be ready at a moment’s notice to act,” says Skipper.

Organizations are also implementing new security tools, with top priorities including:



Despite these strides, overall well-being continues to plague IR teams. Fifty-one percent of respondents to our survey report experiencing symptoms of extreme stress or burnout in the past 12 months. Of those, 67 percent had to take time off work because of it, while 65 percent have considered leaving their jobs altogether.

“Being in cybersecurity is like being an air traffic controller; you’re constantly watching the radar and have to be ready at a moment’s notice to act,” says Chad Skipper, global security technologist at VMware. “Thing is, there are many more incidents in cyberspace than in the airspace, especially in the past year. With stakes this high, it’s no surprise professionals are experiencing burnout.”

To address these issues, organizations should focus on building resilient security teams, McElroy says.

“It’s more important than ever that leaders in this moment take proactive measures to ensure their teams are not only productive but healthy and able to withstand the stresses of the job,” he says. “Those measures could run the gamut, from one-on-ones to hear team members out, to encouraging them to take leadership and professional development courses, to adopting nonstandard activities such as walking meetings and mindfulness training. On the technical side, give your team the time to operationalize a piece of technology before implementing a new one, offer real breaks, and consider rotations of work that assure individuals their careers are progressing.”

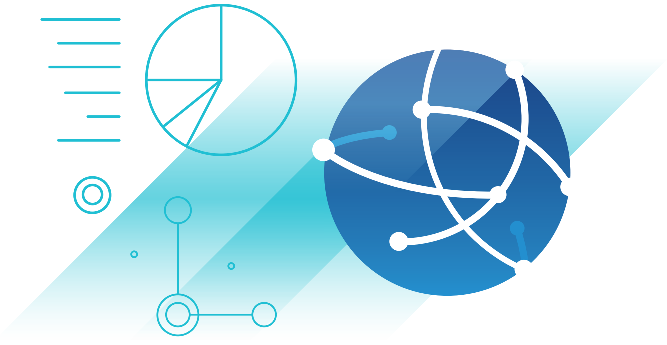
Preparing for the post-pandemic threat landscape

The pandemic ushered in a number of drastic transformations. The shift to remote work led to accelerated cloud adoption, a plethora of business communication platforms, and other new workflow tools. Cybercriminals had the time, opportunities, and capital to collaborate on increasingly sophisticated and damaging attacks. And defenders forced to reckon with it all implemented new ways of fighting back, while struggling to manage extreme stress and burnout.

The impact of COVID-19 continues to take shape in cyberspace. Adversaries are exposing new platforms' vulnerabilities, weaponizing new technologies such as malicious deepfakes, and deploying advanced techniques to deliver integrity attacks that are more targeted and destructive than ever before.

It may feel like we're in the twilight zone. For cybersecurity leaders, the focus must remain on building resilient, cyber-vigilant teams that can proactively detect, prevent, mitigate, and remediate these attacks. More changes are surely ahead in 2021 and beyond. It's up to IR professionals to adapt their defenses as quickly as attackers find new ways to exploit them.

Methodology



VMware conducted an online survey about trends in the incident response landscape in May and June 2021, and 123 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 used in all questions may not add up to 100 percent. To read last year's report, please visit Global Incident Response Threat Report: The Cybersecurity Tipping Point.

Sources

1. The Wall Street Journal. "Kaseya Ransomware Attack: What We Know as REvil Hackers Demand $70 Million." July 6, 2021.

2. The New York Times. "Biden Warns Putin to Act Against Ransomware Groups, or U.S. Will Strike Back." July 9, 2021.

3. The Hill. "Report estimates major cyberattack could cost more than recovering from natural disasters." June 28, 2021.

4. VMware. "Modern Bank Heists 4.0." April 13, 2021.

5. Threatpost.com. "Deepfake Attacks Are About to Surge, Experts Warn." May 3, 2021.

6. Business Insider. "FBI warns of the rise of 'deepfakes' in coming months and explains how to spot them easily." March 29, 2021.

7. VMware. "Global Security Insights Report 2021." June 3, 2021.

8. National Security Agency. "Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments." July 1, 2021.

9. U.S. Secret Service. "Most Wanted Fugitives."

10. Cybercrime Magazine. "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021." October 26, 2020.

11. The United States Department of Justice. "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." June 7, 2021.

12. Cyber Talk. "DOJ assigns ransomware attacks similar status as terrorism." June 4, 2021.

13. BBC. "Nato: Cyber attacks 'as serious as any other attacks' to allies." June 15, 2021.

14. MITRE. "Active Defense Matrix."

15. See 7.

Glossary

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.

Chronos attack – An attack that involves the manipulation of time stamps.

Cloud-jacking – A process in which an organization's cloud account is stolen or hijacked by an attacker.

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.

Integrity attack – An attack launched with the goal of manipulating data.

Island hopping – A technique used by cybercriminals to hijack an organization's infrastructure to attack its customers.

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

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, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com