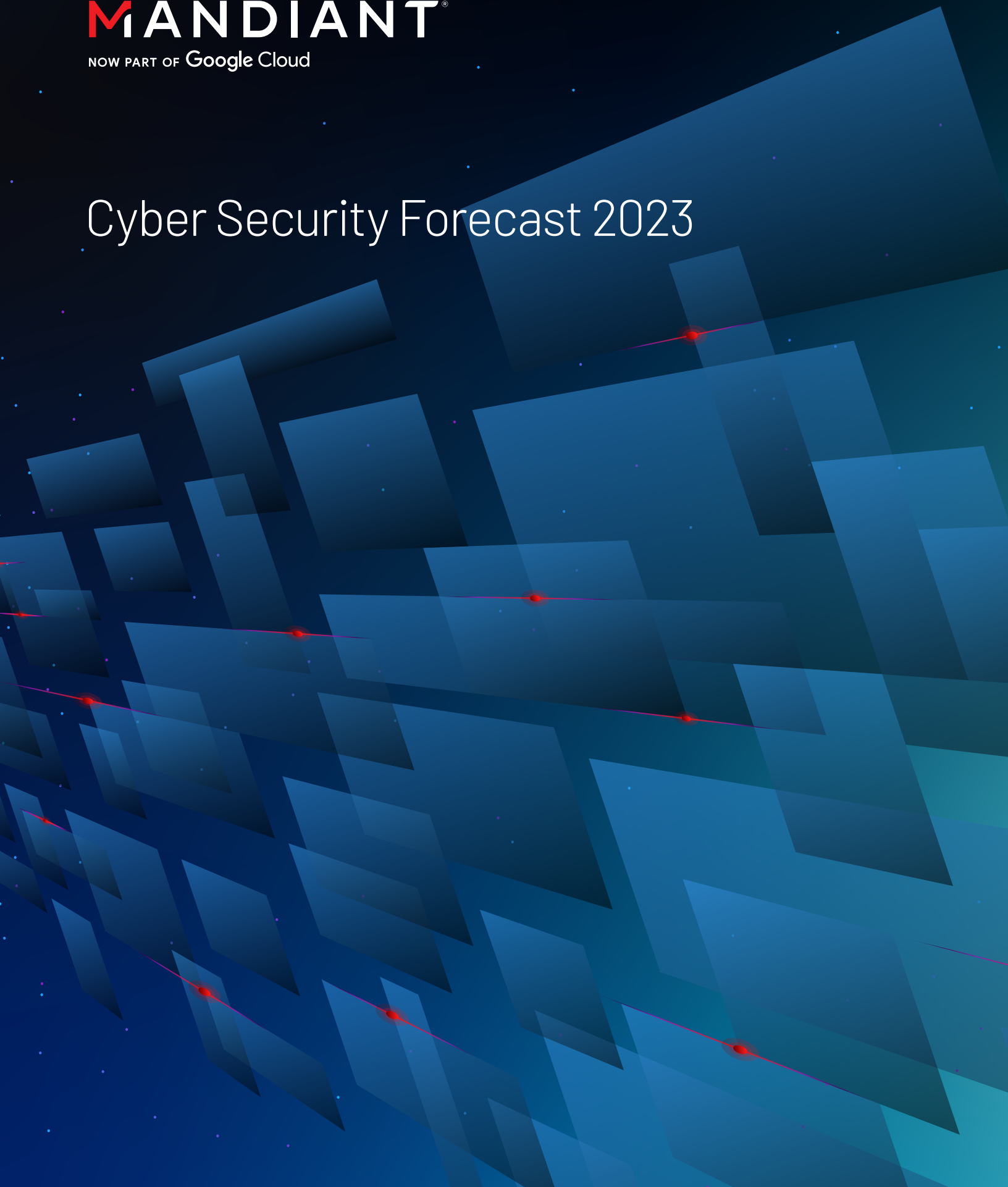
MANDIANT

NOW PART OF Google Cloud

Cyber Security Forecast 2023



Introduction

Our insights on the year ahead have previously been referred to as "predictions." However, our thoughts about the cyber security landscape in the coming year are always based on the trends we are already seeing. "Forecast" captures our intent more precisely. And so, we present the Mandiant Cyber Security Forecast 2023. This report is filled with forward-looking thoughts from several of Mandiant's brightest minds, including Sandra Joyce, Head of Global Intelligence, and Charles Carmakal, Consulting CTO, as well as Phil Venables, CISO for Google Cloud.

Threats evolve, attackers constantly change their tactics, techniques and procedures, and defenders must adapt and stay relentless if they want to keep up. This Forecast aims to help the cyber security industry frame its fight against cyber adversaries in 2023.

Global Forecasts

More Attacks by Non-Organized Attackers and Non-Nation State Attackers

In 2023 we expect to see more intrusions conducted by non-organized attackers and non-nation state attackers. More of the threat actors operating out of North America and Europe will likely be younger, and conducting intrusion operations not because they're interested in making money specifically, or because governments have tasked them with doing it, but because they want to be able to brag to their friends or boast online that they've hacked into and brought embarrassment to prominent organizations. While they will be happy to achieve financial gain, that may not necessarily be their lead motivation.

Europe May Surpass the United States as the Most Targeted Region for Ransomware

Ransomware continues to have a significant impact on businesses across the globe. While reports show that the U.S. is the country most targeted by ransomware attacks worldwide,[1] small indicators show that ransomware activity is decreasing in the United States and growing in other regions.[2] In Europe, the number of victims is increasing, and if that increase continues, Europe will likely become the most targeted region in 2023. The United States has been very outspoken on policies, sanctions and the potential of a response in the cyber domain concerning ransomware and other attacks. However, it is hard to conclude if the more aggressive stance on ransomware actually deters attacks.

More Extortion, Less Ransomware

Historically, cyber criminals have used ransomware to monetize access into a victim's network. Due to several high-profile and visible breaches last year, organizations see mitigating brand damage as a much more compelling reason to pay a ransom than regaining access to encrypted systems. Over the next year, we will continue to see criminals rely on extortion, but actual ransomware deployments may decline. Ransomware-as-a-service (RaaS) providers will modernize their software to focus on data exfiltration and "leak sites" for public shaming.

1. FCW (September 27, 2022). The U.S. is the top target of ransomware attacks, report says.
2. Washington Post (August 17, 2022). Is the drop in ransomware numbers an illusion?.

The Big Four

Russia Cyber and the Invasion of Ukraine

Russia's invasion of Ukraine created unprecedented circumstances for cyber threat activity. This likely is the first instance in which a major cyber power has conducted disruptive attacks, cyber espionage and information operations concurrently with widespread, kinetic military operations. Mandiant anticipates future disruptive attacks in Ukraine and suggests that they are likely to be accompanied by concurrent information operations. We expect that Russia's willingness to use disruptive tactics as well as false or coopted hacktivist fronts—to claim credit for data leaks and data destruction—to increasingly expand outside of Ukraine and its immediate neighbors.

Chinese Cyber Assertiveness

Chinese cyber espionage poses a high-frequency and high-magnitude threat to organizations globally, both in the public and private sectors. Key drivers of Chinese cyber threat activity will include territorial integrity and internal stability, regional hegemony, and expanding global political and economic influence. Cyber espionage and information operations activity in support of China's national security and economic interests will continue to escalate. In 2022, a pro-People's Republic of China (PRC) information operations campaign directly targeted commercial entities in an industry of strategic significance to Beijing.[3] We consider this broader targeting of private sector entities to be notable, and we may see global competitors to Chinese firms in other industries targeted by such information operations.

Iranian Escalation

Mandiant expects that Iranian cyber espionage groups will continue to conduct widespread intelligence collection activity, particularly against government and Middle Eastern targets, as well as telecommunications, transportation and other entities. We anticipate Iranian threat actors' continued willingness to use disruptive and destructive cyber attacks to remain elevated, absent a significant change to Iran's current international isolation.

North Korea Desires Revenue and Intelligence

We assess with high confidence that North Korea will continue to pursue operations that support the regime with both revenue streams and strategic intelligence. International political and economic isolation along with public health challenges will likely inform North Korean cyber espionage against diplomatic, military, financial and pharmaceutical targets. We expect activity to be focused primarily on South Korea, Japan and the United States, with operations also noted in Europe, the Middle East and North Africa, and South Asia.

3. Mandiant (June 28, 2022). Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance.

Information Operations (IO) Will Rely More on Third Party Organizations for Plausible Deniability

Historically, IO have always been politically motivated and state sponsored, as we observed in the 2016 U.S. elections.[4] Since then, we have observed more outsourcing of IO work by state actors. This could be a growing trend in 2023 as "hack-for-hire" engagements become more common. In 2019, OSINT researchers observed a pro-Indonesian IO social media campaign conducted by Jakarta-based media company InsightID.[5] This campaign was aimed at distorting the truth about events in the restive Indonesian province of Papua. Coincidentally supporting this observation, Meta testified in mid-2021 about an increase of hiring marketing or public relation firms in IO campaigns—to lower the barrier of entry for some threat actors and obfuscate the identities of more sophisticated ones.[6]

Enterprises Will Lean into Password-less Authentication

Corporate credential theft continues to be one of the top ways cyber criminals access victims. Furthermore, in 2022, there have been several examples of attackers finding ways to circumvent multi-factor authentication technologies. Apple, Google and Microsoft have committed to consumer-based password-less resources based on standards from the FIDO Alliance and World Wide Web Consortium.[7] The initial roll out of these technologies will focus on consumer-grade password-less resources, but CISOs will demand enterprise identity platforms to expand password-less concepts to the enterprise market. Over the next year, look for enterprise-focused password-less solutions.

Identity First, Identity Lost

Threat actors have shifted from gaining control of an endpoint to gaining access to a user's credentials and account. A user's identity within an organization has become more critical than access to the user's endpoint. Over the next year, we will see threat actors find new ways to steal identities from users using a combination of social engineering, commodity information stealers and information gathering from internal data sources post-compromise. They will combine stolen credentials with new techniques to bypass multifactor authentication (MFA) and abuse Identity and Access Management (IAM) systems.

4. U.S. Department of Justice (March 2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election.
5. Australian Strategic Policy Institute (October 15, 2019). Joint BBC-ASPI investigation into West Papua information operations.
6. ZDNET (July 29, 2021). Disinformation for hire: PR firms are the new battleground for Facebook.
7. Apple (May 5, 2022). Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless sign-ins.

Attackers Will Read More Security Research to Learn Offensive and Defensive Tactics

A trend observed in 2022 is expected to increase: Threat actors will continue to study the blogs and research of analysts in the security community. They will do this to learn offensive tactics and techniques, defensive strategies and how to exploit vulnerabilities. They may discover clever ways to break into organizations, or perhaps learn techniques that were written about in a security post two or three years ago, but that haven't really been used in the wild. We have already observed threat actors reading security blogs from defenders to learn ways they could be detected.

Cyber Insurance Will Be Harder to Obtain and Coverage May Be Restricted

More enterprises have relied on cyber insurance to cover their cyber risks over the years as management has become more aware of cyber security risks. However, claims have also skyrocketed, forcing insurance firms to reevaluate their risk appetite and scale back coverage accordingly. Many firms attempting to renew their cyber insurance—or fresh in the market for cyber insurance—may find difficulty obtaining the coverage they desire.

Widespread Rise of Infostealers and Credential Harvesting

Credential theft leads to impactful intrusions. Mandiant has consistently seen credentials used in intrusions available via infostealers such as REDLINESTEALER, VIDAR and RACOONSTEALER. These stealers are widely available on the underground and purchasing credentials is an inexpensive alternative to trying to phish them from victims. More reporting of initial access brokers in forums and elsewhere (where attackers sell access once they have successfully exploited an entry point), as well as sale of credentials/cookies, will increasingly be used to gain access to organizations with lower cost, complexity and time.

When the Real World Meets the Virtual World

We have already observed and encountered SMS attacks, email attacks and application redirection attacks. Now we see a new model coming—an approach that consists of deceiving victims in the real world. For example, in 2022 we observed a campaign in which victims received a receipt for the delivery of packages in their physical mailboxes. The receipt included a QR code directing them to an identity and credit card number theft site. In 2023, we expect to see more schemes like this, where the attacker uses everyday physical support to deceive their victims. Fake advertisements, fake USB keys, fake receipts—the possibilities for attackers are endless. Educating employees and the public is the best defense against these types of threats.

Further Federal Emphasis on Protecting National Technical Infrastructure Against Malicious Activity

In 2023 we expect to see the Biden Administration implement a consistent stream of policies following the *2021 Executive Order on Improving the Nation's Cybersecurity*[8] *and the 2022 National Security Memorandum.*[9] Although public and private sector collaboration has grown recently, deeper coordination between agencies and big tech organizations is required. We expect the government may implement more safeguarded checkpoints for organizations to reflect on how they have progressed to meet regulatory requirements. As such opportunities are established, we can expect to see more knowledge-sharing between public and private organizations, heightening transparency and protection around the latest impactful threats.

8. The White House (May 12, 2021). Executive Order on Improving the Nation's Cybersecurity.
9. The White House (January 19, 2022). FACT SHEET: President Biden Signs National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.

APJ Forecasts

Cyber Activity Around Southeast Asia Elections in 2023

Several Southeast Asian countries have general elections scheduled for or expected in 2023. We are preparing for the Cambodian general election, Malaysian general election, Myanmar general election and Thailand general election. Cyber espionage groups have had interest in previous Southeast Asian elections and the 2023 elections may prove to be compelling targets. We also expect to see these elections being used as lures for phishing and social engineering. Philippine elections were held in 2022 and the government cited 20,000 attempts to attack the automated election systems.[10]

Asia Pacific Countries Could See More Retaliatory Attacks by Pro-Russia Hacktivist Groups

In 2023 we expect to see more attacks by Russia against entities in Asia Pacific. Since the Russian invasion of Ukraine in early 2022, multiple Asia Pacific countries have enacted sanctions on Russia and in response, Russia has listed multiple countries in Asia Pacific as "unfriendly". When that happened, it raised concerns in the Asia Pacific region because Russian nexus actors were known to conduct retaliatory cyber attacks against international organizations—the PyeongChang Olympics in 2018 was one such case. The targeting of organizations in Asia Pacific represents a significant escalation and expansion in targeting and Asia Pacific-based organizations should also prepare themselves for similar kinds of attacks in the coming months.

Elevated Threat Levels and Disruptions to Semiconductor Manufacturers in Asia Pacific

Disrupted supply chains may introduce additional security risks for semiconductor manufacturers, such as greater vulnerability to a ransomware infection. Available data[11] highlights that the critical manufacturing sector, including the semiconductor industry, continues to be frequently targeted by ransomware. Semiconductor producers are more likely to pay ransoms to prevent monetary losses from production downtime or large-scale work stoppages. These risks, combined with current Sino-American geopolitical tensions, may cause further cyber disruptions to the semiconductor industry in 2023.

10. CNN Philippines (May 11, 2022). Govt blocks over 20K attempts to hack elections, says Esperon.
11. Recorded Future (September 29, 2022). Semiconductor Companies Targeted by Ransomware.

EMEA Forecasts

Russia to Expand Targets Across Europe

A significant portion of Russian cyber activity has been focused on Ukraine since the onset of the conflict, but 2023 could see Russia further expand its cyber operations across Europe. The winter months will likely slow the pace of physical conflict, which could provide Russian cyber threat actors with more threat capacity. During the past year, Russia has typically conducted information-gathering campaigns against European organizations outside Ukraine while most of its disruptive and destructive attacks have been focused within Ukraine. This may change in 2023, with Russia using more of its (potentially increased) disruptive cyber capabilities against European organizations. This could impact a range of organizations, including energy and military suppliers, logistics companies involved in the supply of goods to Ukraine and organizations involved in the introduction and implantation of sanction regimes.

European Energy Concerns to Play Out in the Cyber Realm

Concerns around energy supply and prices within Europe are likely to manifest as malicious cyber operations. Mandiant has already observed an uptick in energy-themed phishing campaigns. Ransomware groups are known to target sectors under pressure, as shown through remorseless healthcare targeting during the pandemic.[12] European energy companies could face elevated targeting during the coming winter months.

European energy suppliers are also a target for Russian state-sponsored threat actors looking to impose further pressure on countries involved in Russian sanction regimes or seeking to reduce their reliance on Russian energy. Pressure on the European energy supply will also increase interest in non-European energy providers. The availability of oil and gas, price movements planed by organizations such as OPEC, and developing government energy policies will all become more important collection targets for state intelligence agencies.

The energy crisis in Europe may also result in more targeting of critical infrastructure. Critical infrastructure is already at risk of destructive cyber attacks when nations are in conflict, but the energy crisis amplifies the threat. We could see critical infrastructure being targeted in ransomware campaigns focused on disrupting energy and power supply.

12. The Verge (August 19, 2021). The pandemic revealed the health risks of hospital ransomware attacks.

Conclusion

Ransomware has been a staple of Mandiant reports for several years, and for good reason. While it is well-established as part of many threat actors' toolkits, data shows more of drop in the U.S. ransomware incidents and a rise in European ransomware incidents. While entities in European regions need to stay especially vigilant, organizations around the world need to be ready for increased attempts at extortion. Extortion actors will stop at nothing to achieve their goals, even using physical devices and less common types of social engineering.

Next year is also expected to bring an increase in the number of attackers motivated simply by bragging rights. These actors are often younger and not tied to a nation state or organized group. However, that doesn't mean we won't see nation-state activity. The Big Four—Russia, China, Iran and North Korea—will be highly active in 2023, using destructive attacks, information operations, financial threats and more.

The road to stronger cyber defenses has never been simple, especially for security professionals. Organizations have a lot to keep in mind for 2023. As always, Mandiant's relentless work on the frontlines gathers insights and develops best practices we regularly share with security leaders, so they can take the steps needed to prevent these threats—and respond quickly and effectively to the attacks that invariably get through.

Contributors

In the past few years of publishing Mandiant Cyber Security Forecast (formerly Security Predictions), Sandra Joyce, Head of Global Intelligence, and Charles Carmakal, Consulting CTO, have spearheaded the report. This year we added insights from Phil Venables, CISO for Google Cloud. Many other experts at Mandiant also contributed to this report, including:

Geoff Ackerman
Jamie Collier
Vivek Chudgar
David Grout
Emiel Haeghebaert
Sarah Hawley
Scott Henderson
John Hultquist
Isif Ibrahima
Jeff Johnson
Igors Konovalovs
Steve Ledzian
Yihao Lim
Keith Lunden
Brendan McKeague
Jens Monrad
Jake Nicastro
Parnian Najafi
Dan Perez
Fred Plan
Clayton Quinlan
Alice Revelli
Nick Richard
Marcin Siedlarz
Matt Shelton
Lindsay Smith
Genevieve Stark
Josh Stern
Van Ta
Kelli Vanderlee

Learn more at www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Industry-leading Mandiant threat intelligence and expertise drive dynamic security solutions that help organizations develop more effective programs and instill confidence in their cyber readiness. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud