MANDIANT

SECURITY PREDICTIONS 2022

14 CYBER SECURITY PREDICTIONS FOR 2022 AND BEYOND

A REFRESHED, REALISTIC OUTLOOK

Although our lives were upended in 2020, the cyber security industry came back strong in 2021. Mandiant rose to the challenge of working under everchanging circumstances while continuing to provide customers with the premium services they associated with our experts.

In cyber security, expectations are critical. One thing we can always count on is the level of uncertainty in the cyber realm. Attackers regularly change their tactics, techniques and procedures (TTPs) to evade detection, leaving defenders struggling to keep up. When Mandiant helps reduce that gap by sharing our informed, evidence-backed learnings and expectations, we also advance the Mandiant mission: to make every organization secure against cyber threats and confident in their readiness.

This year's report, *14 Cyber Security Predictions for 2022 and Beyond*, features more than a dozen insights from our leaders and foremost experts located all around the globe, including Sandra Joyce, EVP, Global Intel & Advanced Practices, and Charles Carmakal, SVP and Chief Technology Officer.

Turn the page to explore the 2022 Mandiant security forecast.

RANSOMWARE AND MULTIFACETED EXTORTION IN THE SPOTLIGHT

1. No End in Sight: Increased Frequency and Expanding Tactics

The ransomware threat has grown significantly throughout the past decade and it will continue its upward trend. The business of ransomware is simply too lucrative, unless international governments and technology innovations can fundamentally alter the attacker cost-benefit calculation. While we have seen efforts to disrupt operations and hold threat actors accountable, cyber criminals simply sign up with another platform—as part of the ransomware-as-a-service business model—to continue their operations. Many ransomware actors are operating from locations not governed by U.S. law, and from regions where their actions don't have as many costs or repercussions. We expect to see more ransomware attacks coming from outside the U.S. We also expect to see an increase in ransomware incidents against critical industries, where the urgency to pay is greater to avoid significant impact on the health and well-being of civilian populations.

Threat actors engaged in multifaceted extortion will continue to find more ways to extort payments from their victims. Multifaceted extortion begins with locking victims out of their own files through encryption (classic ransomware), then adding threats such as making sensitive data public. In 2022 we expect to see actors ramp up new tactics, such as trying to recruit insiders within their victims or targets. We also expect to see more cyber criminals punishing victims that hire professional negotiation firms to help reduce the final amount of the extortion payment. In fact, we have already seen these tactics in 2021, and next year we expect them to evolve as threat actors become more business savvy and learn what kind of situations their victims most want to avoid.

Threat actors engaged in multifaceted extortion will continue to find more ways to extort a payment from their victims.

2. No Honor Among Thieves: More Disputes Between Threat Actors

Ransomware-as-a-service operations regularly involve multiple actors, each one performing a specific element of the attack for a fee or a cut of the proceeds. We anticipate that there will be increased conflict amongst these actors throughout 2022, and that this conflict may ultimately lead to bad outcomes for victims. Conflicts may occur when targets don't pay, or if law enforcement disrupts threat actors' ability to get paid. Conflicts may also occur when victim organizations do end up paying; a specific actor may feel they didn't get paid enough or that they're not getting their fair share. We are already seeing this type of conflict between actors and victims could suffer for it. In the next 12 months we expect to see many situations where victims will pay a million dollars or more to keep their stolen data from being published. In some of these situations, some or all that data may be published by one of the actors in the operation because of conflict. The more this happens, the more it's going to affect the way organizations think about making ransom payments.

3. Organizations Caught between U.S. Government and Ransomware Actors

The U.S. government is focused on ransomware and how to curb it, and this may lead to negative consequences for organizations. For example, U.S. organizations—and organizations that are not based in the U.S., but do business in the U.S.—are not allowed to pay sanctioned threat actors or any group or individual on the United States Department of Treasury no-pay list. Even so, in a few public cases, victims paid groups that may have had some loose connectivity to sanctioned entities—not necessarily guaranteed connections or even concrete connections, but some loose beliefs that there might have been a connection. We suspect that the government may make an example of one or more large organizations that make a payment to a suspected sanctioned entity, just to try to curb and stop victim organizations from paying large extortion demands. There are several different perspectives on extortion payments, including banning them outright to make the whole process illegal. Consequently, we anticipate there will likely be some negative recourse to a victim organization that paid an extortion demand.

Many OT devices are not built with security at the forefront of the design.

4. Cyber Physical Systems Increasingly Under Threat from “n00bs”

Throughout 2021, we observed low sophistication threat actors learn that they could create big impacts in the operational technology (OT) space—perhaps even bigger than they intended. Actors will continue to explore the OT space in 2022 and increasingly use ransomware in their attacks. This targeting will occur because of the need to keep OT environments fully operational, especially when the systems are part of critical infrastructure.

Attacks against critical OT environments can cause serious disruption and even threaten human lives, thereby increasing the pressure for organizations to pay a ransom. To compound the issue, many of these OT devices are not built with security at the forefront of the design, and we’re currently seeing a massive uptick in the number of vulnerabilities being identified in OT environments.

5. More Public Breaches in the Asia-Pacific and Japan (APJ) Region

Historically, breaches in the APJ region have not been made public, but that is likely to change in 2022 as multifaceted extortion becomes more prevalent. In the past, making the public aware of a breach benefitted neither the attacker nor the victim organization. The attackers wanted to stay invisible for as long as possible, hoping to maintain their access to victim networks for extended periods of time. And victims wanted to avoid the reputational damage, financial impact and other consequences that come from a breach. Multifaceted extortion has changed all that. Now attackers are simply threatening to expose breaches and publish sensitive data to increase urgency to pay. APJ organizations must be ready to deal with these types of extortion operators, but unfortunately many in the region lack experience with these types of threats, or don't take them seriously. Therefore, we expect to see a lot more breaches of APJ organizations being made public by attackers.

OUTLOOK ON MAJOR NATION-STATE ACTORS: THE BIG FOUR

6. Russia

Russia will maintain an aggressive posture throughout the remainder of 2021 and into 2022, with a sustained emphasis on targeting NATO, Eastern Europe, Ukraine, Afghanistan and the energy sector. The U.S. government attributed the UNC2452 attack (also referenced as the SolarWinds supply chain compromise incident) to Russia, which demonstrates Russia has the ability to achieve widespread impact. We expect supply chain and software supply chain environments to continue to be targeted by Russia next year. Additionally, UNC2452's manipulation of authentication methods in hybrid cloud/on-prem environments highlights innovative tactics, leading us to believe the level of sophistication and scope of Russian operations will expand.

7. Iran

Iran will use its cyber tools in a much more aggressive manner to promote regional interests. Information operations attributed by the U.S. to Iran in 2020 and 2021 demonstrated more aggressive tactics than previously seen. Iran will also continue to target Israel and others in the Middle East. They've shown their capability and willingness to use destructive malware, so we expect them to take advantage of any opportunities that are presented. Ultimately, we'll see Iran trying to create more of a power balance shifted to its own interests. We have seen them targeting abroad, but their targeting will most likely be regional throughout 2022.

8. China

China will continue to be very aggressive, supporting the Belt and Road Initiative using cyber espionage. Now that the Ministry of State Security (MSS) and the People's Liberation Army (PLA) have completed most of their reorganization, their operations are going to become much more focused. China has shown a willingness to scale their operations and take steps that they were previously unwilling to take. As geopolitical tensions continue to rise, the big question is "When are we going to see China flex some of their known but as-yet-unused destructive capabilities?"

9. North Korea

North Korea, with its geographical, international and financial challenges, is willing to take a lot of risks. In 2022, we expect to see North Korea flex its cyber capabilities to make up for its lack of other instruments of national power. The North Korean cyber apparatus will continue to support the Kim regime by funding nuclear ambitions and gleaning strategic intelligence.

10. EVENTS IN AFGHANISTAN TRIGGER ESPIONAGE AND INFORMATION OPERATIONS

With the assertion of Taliban control and departure of U.S. forces from Afghanistan, we can expect further cyber espionage and information operations. We will start to see the usual information operations actors—Iran, China, Russia—push narratives to support their interests through the end of 2021 and into 2022. They'll also play up negative perceptions around the events, notably the perception that the U.S. failed to live up to its commitments to organizations and countries. The declaration of an Emirate may also embolden pro-Islamist extremist actors to expand propaganda activities, including hacktivist tactics such as defacements, social media account takeovers and dissemination of "kill lists" compiled from open source or compromised data.

Deepfakes have been used to facilitate BEC fraud, bypass MFA protocols and KYC ID verification.

11. DEEPFAKES: NOT JUST FOR INFORMATION OPERATIONS

The effectiveness of deepfakes in information operations has been discussed in the security community, but state sponsored and financially motivated actors have also demonstrated growing interest in this technology. Mandiant observed posts and advertisements about deepfake technology in underground Russian and English language criminal forums throughout 2020 and 2021. Users on these underground forums advertised customized deepfake videos and images, as well as training for users to create their own manipulated media. Deepfake audio has facilitated business email compromise (BEC) type fraud schemes. Open sources highlight how threat actors have used manipulated media to bypass multi-factor authentication (MFA) security protocols and Know Your Customer (KYC) identity verification measures. We anticipate that as deepfake technology becomes more widely available in 2022 and beyond, criminal and espionage actors will increasingly integrate manipulated media into their operations to make social engineering more convincing, easily tailor content to specific targets and defeat some automated identity verification systems.

12. CYBER OUTSOURCING INCREASES VELOCITY AND IMPACT OF MALICIOUS OPERATIONS

Outsourcing in malicious operations via mechanisms such as ransomware affiliate programs, exploit vendors, commercial contractors, malware vendors and freelancers contributes to both the increasing frequency and complexity of cyber threat activity. We see no signs that this will slow down in 2022. Blurring distinctions between financially motivated and state-sponsored operations in terms of both tools and talent, maturing legitimate and illegitimate markets for third-party tools and services, and growing specialization and commodification of cyber threat skills—particularly in cyber crime communities—all contribute to making more sophisticated capabilities accessible to a wider pool of nation-state sponsors and criminal actors. For defenders, this translates to increased overall cyber risk as the quantity, quality and adaptability of malicious operations grows. It also complicates attribution, tracking and distinguishing activity sets, as well as the development of defensive strategies focused on actor motives and TTPs.

The proportion of Mandiant incident response investigations involving cloud resources has grown over the past several years.

13. CLOUD AND THIRD PARTIES INTRODUCE NEW CHOKEPOINTS

Organizations will continue to increasingly rely on cloud and cloud-hosted third-party providers for primary business tasks, putting more pressure on those third parties to maintain both availability and security. If either of those features are disrupted, organizations must be prepared to work around interruptions and diagnose, address, and recover from an incident when they may have not been the primary target and may not have access to the full picture of the attack lifecycle in internal logs. The proportion of Mandiant incident response investigations involving cloud resources has grown over the past several years. We anticipate that cloud compromise and abuse will continue to grow in tandem with enterprise cloud adoption throughout 2022. We suspect that organizations using cloud and cloud-hosted providers may become more vulnerable to compromises, as well as errors, vulnerabilities, misconfigurations or outages affecting cloud resources.

14. MORE INTERNET OF THINGS DEVICES, MORE VULNERABILITIES, MORE ATTACK SURFACE

In the coming years, we expect to see a continued growth of Internet of Things (IoT) devices, many of which will be inexpensive and created without real consideration given to security. The number of vulnerabilities they introduce—in software and hardware—will make it hard for bug hunters to keep up. Because all these devices are connected, we'll see the general attack surface expand with the potential for serious impact. Unfortunately, there hasn't been enough emphasis on security in fundamental IoT device design to fix these issues, so the situation will only get worse in the years to come. When fixes are released for newly discovered vulnerabilities, the user must take the initiative to update their devices. Most users may never be aware that an update is required, and if they do, they may not even care. There has been no coordinated security initiative for IoT devices. Technologies such as Secure Boot are helping, but they are only being implemented by larger organizations and in newer products. It is true that companies such as Microsoft and Amazon are creating platforms that will provide smaller companies with an opportunity to build more secure IoT devices. These are steps in the right direction, but it will take several years before a secure IoT landscape is realized.

There has been no coordinated security initiative for IoT devices.

PURSUING A MORE SECURE FUTURE

‘Predictions’ may pack more punch, but in cyber security, ‘forecasting’ is perhaps more appropriate. That’s because our expectations of the future are based on the trends we see now. And it’s not just the attacker behaviors; we consider everything else, from technology and workplace trends to changing laws and regulations.

Every recent Mandiant predictions report has included a section on ransomware. This year is no exception; in fact, our outlook on the threat for 2022 is perhaps more grim. Ransomware actors are becoming increasingly aggressive, turning these once relatively simple attacks into more elaborate—and lucrative—multifaceted extortion operations. U.S. and international efforts against ransomware are underway, but they have not affected the ransomware-as-a-service business model. In a cruel twist, government efforts could lead to negative outcomes for organizations.

Ransomware isn’t going anywhere, and neither are espionage and information operations. In 2022, we will continue to see regional and international activity conducted by the Big Four: Russia, Iran, China and North Korea. We will also see this type of activity stemming from recent events in Afghanistan. Increased use of deepfake technology will only compound the threats.

Organizations have a lot to keep in mind in 2022, but remaining vigilant will enable them to defend against upcoming threats—and respond to those that inevitably get through. Mandiant, incorporating the broadest and deepest cyber expertise and threat intelligence into dynamic cyber defense technologies, will help empower them.

Learn more at **www.mandiant.com**

Mandiant
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT