WHITE PAPER

Cyber Threat Predictions for 2021

An Annual Perspective by FortiGuard Labs

Introduction

Each year at this time, we take a look at trends across the technology landscape to predict emerging security issues, whether just around the corner or further afield. Predicting security threat trends may seem like more art than science, but the reality is that combining a strong understanding of how threats develop and what sorts of technologies cyber criminals gravitate toward (both to use and to exploit) with evolving business trends and strategies helps make predictions a reasonably straightforward process.

Threat actors are shifting significant resources to target and exploit emerging network edge environments, such as remote workers and the cloud.

However, this also requires having spent years identifying and assessing cyber-criminal activities and behaviors, working closely with law enforcement to track down and catch criminals, and building strategies designed to thwart malicious activity. And the cybersecurity threat researchers at FortiGuard Labs have spent the last 20 years doing just that. While some of the details may change, attack patterns, criminal behaviors, and objectives are relatively constant when seen through the lens of experience. Mapping these predictable behaviors against technology trends yields critical insights into the sorts of things organizations need to be preparing for if they want to protect their connected resources from tomorrow's cyberattacks. These include the theft of data and intellectual property, evolving ransomware techniques, device compromise, social engineering, and other looming digital threats.

Over the past several years, this annual predictions report has touched on such issues as the evolution of ransomware, the risks of an expanding digital business footprint, and the targeting of converged technologies—especially those that are part of smart systems such as smart buildings, cities, and critical infrastructures. It has also considered the evolution of morphic malware, the grave potential of swarm-based attacks, and the weaponization of artificial intelligence (AI) and machine learning (ML). Some of those have already come to pass, and others are well on their way. To get out ahead of these challenges, organizations need to do two things: first, stay abreast of ongoing trends, and second, begin preparing now to defend against these emerging threats.

Living on the Edge

Over the past few years, networks have been radically transformed. In simplest terms, the traditional network perimeter has been replaced with multiple edge environments—local-area network (LAN), wide-area network (WAN), multi-cloud, data center, remote worker, Internet of Things (IoT), mobile devices, and more—each with its unique risks and vulnerabilities. One of the most significant advantages to cyber criminals in all of this is that while all of these edges are interconnected, often due to applications and workflows moving across or between multiple environments, many organizations have sacrificed centralized visibility and unified controls in favor of performance and agility.

Threat actors are shifting significant resources to target and exploit emerging network edge environments, such as remote workers and the cloud, rather than just targeting the core network. Securing these new environments, including new technologies and converging systems, is more challenging than it may seem. The transition to remote work, for example, is not just about more end-users and devices remotely connecting to the network. While we have seen an expected spike in attacks targeting novice remote workers and vulnerable devices to gain network access, we are also beginning to see new attacks targeting connected home networks. Much of that effort is focused on exploiting older, more vulnerable devices such as home routers and entertainment systems. But there are also new efforts underway targeting smart systems connected to the home environment that tie multiple devices and systems together.

Smart devices that interact with users, such as AI-based virtual assistants, collect and store volumes of information about its users. Compromising such devices can yield valuable information that can make social engineering-based attacks much more successful. And as these devices begin to control more elements of our lives, successfully compromising such a system can lead to such things as turning off security systems, disabling cameras, and even hijacking smart appliances and holding them for ransom.

But that is just the start. While end-users and their home resources can be compromised through the exploitation of detailed information, more sophisticated attackers use these as a springboard into other things. Corporate network attacks launched from a remote worker's home network, especially when usage trends are clearly understood, can be carefully coordinated so they don't raise suspicions. Intelligent malware that has access to stored connectivity data can much more easily hide. But that's just the start. Advanced malware can also sniff data using new Edge Access Trojans (EATs) to do things like intercept voice requests off the local network to compromise systems or inject commands. Adding cross-platform capabilities to EAT threats through the use of a programming language like Go will make EATs even more dangerous as these attacks will be able to hop from device to device regardless of the underlying OS.

Competing against the deep security resources of large organizations puts cyber criminals at a disadvantage. To succeed, cyber criminals need to leverage resources laying around at their disposal—the low-hanging fruit. But increasingly, these edge devices will also be leveraged for ML, especially as they are increasingly powered by 5G and beyond. By compromising edge devices for their processing power, cyber criminals will be able to surreptitiously process massive amounts of data and learn more about how and when edge devices are used. Compromising edge devices can enable things like cryptomining much more effectively than traditional monolithic systems. Infected PC nodes being hijacked for their compute resources are often noticed quickly since CPU usage is high and directly applies to the end-user's workstation. Compromising secondary devices would be much less noticeable. As a result, visibility on other health metrics for these devices will become more critical—especially as edge devices and an expanding number of edge networks begin to play a more crucial role in corporate networks. But for many organizations, by the time they implement an edge computing strategy, the devices they will rely on will have already been compromised.

Advanced malware can also sniff data using new Edge Access Trojans (EATs) to do things like intercept voice requests off the local network to compromise systems or inject commands. Adding cross-platform capabilities to EAT threats through the use of a programming language like Go will make EATs even more dangerous as these attacks will be able to hop from device to device regardless of the underlying OS.

Compromising and leveraging 5G-enabled devices will also open up new opportunities for advanced threats. Over the last several reports, we have been documenting the progress made toward developing and deploying swam-based attacks. Swam attacks leverage thousands of hijacked devices divided into subgroups with specialized skills. They target networks or devices as an integrated system and share intelligence in real time to refine an attack *as it is happening*. This increases the efficiency and effectiveness of their attack. Swarm technologies require large amounts of processing power to power individual swarmbots and efficiently share information between the different members of a swarm. This enables them to more rapidly discover vulnerabilities, share and correlate those vulnerabilities, and then shift attack methods to better exploit them. These networks will also be needed to power and enable AI-based systems so that coordinated attacks can rapidly become more efficient and effective at both compromising systems and evading detection.

To make all this happen, AI will need to evolve to the next generation. This will include leveraging local learning nodes powered by ML. Such nodes will also need to have analysis and action capabilities and the ability to speak with and update each other with what they see. These advances in AI are already in motion. In the meantime, we can expect to see an increasing number of open-source toolkits designed to help cyber criminals effectively target and compromise edge devices. These tools will also help cyber criminals create and maintain ad hoc networks of compromised devices to ensure large amounts of computing power are available at a moment's notice. This will enable them to more effectively launch attacks, overcome security systems, and avoid countermeasures. The addition of advanced AI by some well-funded cyber-criminal organizations will also allow them to learn how to detect and overcome defensive strategies. In addition, we can also expect a rise in compromised networks of edge devices that are sold as a service. These malicious edge networks could then be used to process information, gather intelligence about a target, or launch a coordinated attack that simultaneously targets as many attack vectors as possible, thereby overwhelming defenses.

Last year, we predicted that the advent of 5G might be the initial catalyst for developing functional swarm-based attacks. We also said that this could be enabled by creating local, ad hoc networks that can quickly share and process information and applications. Today, we seem closer to that prediction than ever before. In the U.S., for example, basic 5G coverage (with a 600 MHz spectrum that's more effective at penetrating buildings and covering long distances) is now available in 5,000 cities and to over 200 million Americans. The much faster millimeter-wave 5G is also being rolled out, starting in six cities, with more on the way. New advances, such as massive multiple-input multiple-output (MIMO) technology, provide uniformly good service to wireless terminals in high-mobility environments. And now, new 5G-enabled smartphones are beginning to include a 5G mmWave antenna to accelerate adoption even faster.

Cyber criminals have not missed the implications or the opportunity for exploitation. By weaponizing 5G and edge computing, individually exploited devices could not only become a conduit for malicious code but groups of compromised devices could work in concert to target victims at 5G speeds. Adding the intelligence provided by connected virtual assistants and similar smart devices means that the speed, intelligence, and localized nature of such an attack may overcome the ability of legacy security technologies to effectively fight off such a strategy.

By weaponizing 5G and edge computing, individually exploited devices could not only become a conduit for malicious code, but groups of compromised devices could work in concert to target victims at 5G speeds.

Exposure: The Rise of AI-based Playbooks To Predict Attacks (or Beat Security Systems)

Combining AI and Playbooks To Predict Attacks

Investing in AI not only allows organizations to automate tasks but it can also enable an automated system that can look for and discover attacks after the fact and before they occur. And one of the most exciting cybersecurity tactics to come out of this is the development and use of playbooks that document the behaviors of malicious attacks and cyber-criminal organizations in detail, an idea we discussed in last year's predictions report.

Today, as AI and ML systems gain a greater foothold in networks, the ability to build and deploy such playbooks is much closer to reality. Basic playbooks using various schemes to document and standardize behaviors and methodologies, such as the MITRE ATT&CK framework, are already being produced by some threat research organizations, including FortiGuard Labs. These threat "fingerprints," or tactics, techniques, and procedures (TTPs), provided by threat-intelligence sources, are fed to AI systems to enable them to detect attack patterns and interrupt attacks by anticipating and shutting down the next step in an attack sequence.

Once this information is added to an AI learning system and augmented through trained ML systems, networks will not need to wait until they are under attack to respond effectively to a threat. Remote learning nodes placed at the edges of the network, and even out beyond the network as reconnaissance sensors, will provide advanced and proactive protection. They will be able to detect a threat and forecast threat actor and malware movements to proactively intervene. They can also coordinate with other nodes to simultaneously detect attack profiles never available before—such as identifying artifacts from attack code, compiler behavior, symbols, and styles associated with advanced persistent threat (APT) groups—to shut down all avenues of attack.

Playbooks can reflect attack patterns and the granularity of malicious behavior—the TTPs of cyber criminals—to enhance threat response and generate attack simulations to strengthen the skills of cybersecurity professionals. This sort of Blue Team training gives security team members the ability to improve their skills while locking down the network. Similarly, as organizations light up heat maps of currently active threats—a graphical representation of real-time cyber risk—intelligent systems can proactively obfuscate network traffic and targets and precisely place attractive decoys along predicted attack paths to attract and trigger cyber criminals. Eventually, organizations could respond to any counterintelligence efforts before they happen, enabling them to maintain a position of superior control.

In this area of cybersecurity development, competing against the deep security resources of large organizations puts cyber criminals at a disadvantage. Threat defenders generally have the lead in this space because they have the budgets and dedicated resources needed to implement things at scale. Cyber criminals not only need massive data and compute resources to get AI to work for them, which they generally don't have, but they also need to invest years in training an AI so it can produce the results they desire. This is cost-prohibitive for most criminal organizations, which is why even the most advanced cyberattacks can still only leverage the most basic kinds of ML and AI solutions, if at all. However, one class of cyber criminals already has the resources needed to leverage such playbooks for themselves, which is adversarial nation-states. In their hands, a playbook can be used to modify an attack so that it evades detection, or tip the hand of defenders by anticipating and undermining countermeasures because they are leveraging the same playbook.

And even this gain may only be temporary. Leveraging vast networks of compromised (primarily edge) devices may enable creative cyber criminals to approximate the computing power of corporate networks. And once that challenge has been resolved, it will only be a matter of time before such resources are available as a darknet service. This means that organizations that lag in the adoption and development of AI-based systems and advanced security playbooks will be more likely than ever to be steamrolled by these tactics.

Ransom Models—Darknet Negotiations, Cyber Insurance

Ransomware continues to evolve, enabling it to continue to be the most dangerous and damaging threat organizations face today. For example, this past year, ransomware developers implemented a new strategy designed to counteract the decision of many organizations to not pay a ransom, but instead to restore compromised systems on their own. What cyber criminals now do, in addition to encrypting data and systems, is to also post that data on public servers. They then not only demand a ransom but also threaten to publicly release valuable intellectual property and sensitive information if their ransom demands are ignored. And some are even going further by extracting sensitive information that could expose an organization or its executives to public shame. Extortion, defamation, and defacement are all tools of the trade that have moved to the digital realm. This includes the emerging focus for law enforcement on sextortion, in which the threatened release of sexual images or information is the means of coercion. Examples of home cameras being targeted, and footage being posted online, are already in the news.

Ransomware continues to evolve, enabling it to continue to be the most dangerous and damaging threat organizations face today.

This game of one-upmanship cannot continue forever. Ironically, there are now organizations popping up on the darknet with a business model of negotiating ransoms. While this may have short-term benefits, such as saving victims money and shortening the ransomware cycle, it also has the chilling effect of normalizing criminal behavior and ensuring that cyber criminals always get a payday.

However, the reality is that ransomware is likely to continue to escalate, and the ramifications will only become more pronounced as hyperconvergence takes hold within networks. As networks, devices, applications, and workflows cross over and through each other to deliver smarter services, more critical processes can be affected by a breakdown anywhere in the network. And as systems increasingly converge with critical infrastructure systems, there will soon be more data and devices at risk. Human lives will be lost when power grids, medical systems, transportation management infrastructures, and other critical resources become targets. A ransomware attack targeting an ICU filled with patients is likely to happen, probably sooner than later, and ransomware will then cross the line between criminal activity and terrorism. In fact, one recent event—where a ransomware attack rendered a hospital IT booking system unable to accept new patients, forcing a patient on an ambulance to take a much longer detour to another hospital, subsequently dying en route—demonstrates the potential for such an attack. Similar events are likely to target critical infrastructure, such as disabling safety controls in a nuclear power plant or opening the floodgates in a dam.

Like the other threats discussed in this report, cyber criminals' ability to continue to escalate the ransomware threat will depend on their ability to leverage and exploit edge and other systems. New edge networks built using vulnerable devices will enable cyber criminals to deploy ML so they can detect vulnerabilities in complex systems, develop malware enhanced with AI to launch sophisticated attacks—such as targeting multiple attack vectors—and approximate the computing power of larger networks to coordinate multiple attack elements simultaneously, such as is needed to manage a swarm-based attack.

Swarm Intelligence

As we said last year, ML and AI continue to enable advances in swarm intelligence. Originally introduced by Gerardo Beni and Jing Wang in 1989, swarm intelligence describes the collective behavior of decentralized, self-organized systems, whether natural or artificial. Inspired by biological systems such as ants, bees, termites, bird flocks, and bacteria, swarm intelligence is being leveraged as a computational tool to optimize complex problems such as vehicle routing, job shop scheduling (JSS), or the "knapsack" problem. The most notorious application of swarm intelligence is the usage of the ant colony algorithm for IP network routing.

The development of swarm intelligence has powerful implications in areas such as the development of new pharmaceuticals and medical procedures, the coordination of complex transportation environments, and a wide variety of automated problem-solving for massive systems run by the military and the aerospace industry.

However, as we have warned repeatedly, swarm intelligence will also be a game-changer for adversaries if organizations do not update their security strategies. When used by cyber criminals, bot-based swarms could be used to quickly overwhelm network defenses, efficiently find and extract critical data, and remove or compromise forensic information.

We already see malware that includes multiple payloads and then selects the appropriate tool for a job based on real-time reconnaissance, but that can also receive instructions to modify its attack based on the data it collects and shares with its command-and-control center. The new HEH Botnet, for example, leverages a proprietary peer-to-peer (P2P) protocol that keeps track of its infected peers and enables the attacker to run arbitrary shell commands. It is written in Go language so it functions cross-platform. It also includes a wiper function that can remove all data from a compromised device by triggering a self-destruct command, something we predicted back in 2017. HEH and similar emerging threats are a good example of how malware authors are shifting from compiled native binaries (e.g., using C) to cross-platform tools like Go.

Eventually, such attacks will be comprised of thousands or millions of specialized bots—clustered according to specific functions—that can up the ante by correlating real-time intelligence during an attack to more quickly and efficiently compromise a target, including overcoming active defense systems.

The only defense against this sort of ultimate attack system is AI-enhanced technologies that can see, anticipate, and counter such an attack, stroke for stroke. The cyber wars of the future will occur in microseconds. The primary role of humans will be to ensure that security systems have been fed enough intelligence to not only actively counter live attacks but actually anticipate those attacks so that they don't happen in the first place.

Security implemented after the fact is never as fast and effective as security woven directly into the technology while still on the drawing board.

Future Threats

One important lesson is that security implemented after the fact is never as fast and effective as security woven directly into the technology while still on the drawing board. One primary concern will be our growing reliance on data and internet links enabled through advanced satellite-based systems such as Starlink. Naturally, satellite security systems have been nominal, primarily because they are so remote, because they run on customized hardware, and only use proprietary operating systems and applications. However, as satellite-based networks proliferate, compromising satellite base stations and then spreading that malware through satellite-based networks, it gives attackers the ability to potentially target millions of connected users.

And as computing power advances, encrypted traffic across these satellite networks will no longer be an effective defense mechanism. Historically, airlines, cruise ships, and military systems have been the ones that have most heavily relied on satellite data. But as complex systems, whether owned by corporations or connected to critical infrastructures, begin to rely on a network of satellite-based systems, what are the implications as cyber criminals begin to target them? This will initially be an OT play, probably starting with things like distributed denial-of-service (DDoS) attacks. But as communications with satellite systems become more common, expect more advanced attacks to quickly follow.

The Quantum Threat

The most forward-looking threat prediction revolves around quantum computing. Many people argue that the nature of quantum computing makes them naturally immune to attack. But what happens when quantum-based devices are aimed at things like breaking cryptographic keys and algorithms?

A quantum computer uses a different method to represent and compute information, allowing it to operate at much, much faster speeds than today's computers. It's not just *evolutionary*, but *revolutionary*. The introduction of qubits, which leverage how an electron behaves when suspended in a magnetic field, enables the exponential amplification of the computing power of a device. In a classical system, a bit is one-dimensional. It is either in one state or the other (on or off). Quantum mechanics, at its simplest, is two-dimensional. This allows a qubit to be in a coherent superposition of both states simultaneously (on, off, *plus* neither on nor off). Put simply, because a classical computer performs computations using bits that can only represent two states, the number of states available for computations only expands linearly (three bits have six states [2+2+2], four bits have eight, etc.). But the number of representational possibilities available to a quantum computer expands exponentially (three qubits have 2^3, or eight states, four qubits have 2^4, or 16 states, etc.).

And that's just the start. Qudits (the "d" representing a variable number of dimensions) take this concept even further. In 2017, for example, scientists at the National Institute of Scientific Research constructed a pair of qudits with 10 different states each, providing more computational power than six qubits. Compound that by millions of qubits (or qudits), and the potential computational power of a quantum computer seems limitless.

From a cybersecurity perspective, quantum computers will play a potentially devastating role in undermining the effectiveness of things like data encryption. Quantum computers will quickly render asymmetric encryption algorithms obsolete. (These are the algorithms used to "sign" information to ensure data integrity, perform key exchanges to enable confidentiality algorithms to scramble data, and to verify authenticity of people or data.) In fact, it is being predicted that quantum computers will break elliptical curve cryptography by 2027.

From a cybersecurity perspective, quantum computers will play a potentially devastating role in undermining the effectiveness of things like data encryption.

Of course, quantum computers are not currently commercially available, at least not to the usual assortment of cyber criminals most organizations are concerned with. However, they still have one colossal benefactor—nation-states. There are numerous nations now that either have quantum computers or that are in the process of developing them. While most of these are being leveraged for the general good, such as medical research, weather forecasting, and solving complex mathematical problems, there has never been an advanced technology that wasn't also coveted by the segments of the government dedicated to things like espionage.

Many governments have long been engaged in a process known as data scraping, collecting mountains of encrypted data from nations and industries in which they have a national economic interest. That information is just sitting there, waiting for the right tools to come along and break the lock.

As a result, organizations will need to shift to quantum-resistant computing algorithms wherever you use cryptography to "sign" information, establish crypto keys for a communication, and protect the integrity of information. Universities, government agencies, and specialized security organizations are now spending significant resources developing advanced cryptography tools around the principle of crypto-agility. According to National Institute of Standards and Technology (NIST) guidelines, "maintaining crypto-agility is imperative" in preparing for the quantum-computing era. Hard-coded cryptographic systems do not allow for protection or efficiency once vulnerabilities are discovered. Instead, technological agility needs to rely on new development frameworks and service software to consistently and seamlessly protect applications and data that rely on strong cryptography.

Organizations need to make "security agility" part of their operational security doctrine. This includes ensuring that security solutions have the ability to seamlessly transition to quantum-resistant asymmetric cryptographic algorithms and quantum key exchange once they are available. NIST is currently developing a "Post-quantum Crypto" standard. Ideally, organizations should seek to adopt a quantum-resistant algorithm several years before quantum computers become generally available, especially those likely to be targeted by state-sponsored espionage.

What Organizations Need To Do

Some organizations are waking up because this new cyber-threat world is real and not going anywhere. They have adopted a new mantra that acknowledges that cyber preparation needs to not focus on "if", but "when" they are a target. That means their resources need to not only be focused on proactive defense but also on effective incident response as well. That's because they understand that a breach is inevitable, and protecting the network depends on knowing what to do next to stop that attack in its tracks.

An effective and integrated next-generation AI system provides the best chance to defend networks and respond to attacks before achieving their objectives. It needs to function akin to the adaptive immune system that protects our bodies from disease, fights off infections once our bodies have been compromised, and modifies that immune system to fight off those same viruses in the future.

Tighter Integration with the Public Sector

Organizations cannot be expected to do all of this on their own. They need to subscribe to threat-intelligence feeds, belong to relevant consortiums, and proactively share data and strategies with others in their region or industry. And they also need to work with vendors who have established close partnerships with public sector institutions, such as law enforcement and education.

A private-public alliance in education will not only help educate future citizens to better protect themselves and engage in safe cyber behaviors that respect and protect society, but it will also help fill the growing cybersecurity skills gap that threatens to take down the emerging digital economy. This should not be limited to post-secondary training but should begin with K-12 schools, encouraging students to join the "good side" before they go dark.

Cybersecurity vendors, threat researchers, and industry leaders must partner with law enforcement, especially now as law enforcement begins to change the scope and scale of their efforts. One of the biggest challenges law enforcement faces is that cyber crime does not respect political borders. The fact is, lots of crime—from harassing phone scams originating from foreign call centers to software piracy to the theft of data or finances—hides behind the protections provided by an international border. As a result, law enforcement organizations have built global command centers closely tied to the private sector, enabling them to see and respond to cyber criminals in real time.

A security fabric must be woven from the solutions and threat intelligence forged through these relationships between law enforcement and public and private sector organizations. This includes subscribing to threat feeds dedicated to enabling security resources and enabling team members to stay abreast of emerging threats. This will help companies identify and respond more effectively to cyber criminals and enable them to create and deploy more effective playbooks to better thwart cyber crime and identify criminals and criminal behavior. Over the next few years, we will see even more Initiatives designed to foster a more unified approach between international and local law enforcement agencies, governments, businesses, and security experts. Together, combined with ongoing advances in cybersecurity technologies, they will be able to expedite the timely and secure exchange of information and response to protect critical infrastructure and against cyber crime and put cyber criminals out of business.

About FortiGuard Labs

FortiGuard Labs is the threat intelligence and research organization at Fortinet. Its mission is to provide Fortinet customers with the industry's best threat intelligence designed to protect them from malicious activity and sophisticated cyberattacks. It is comprised of some of the industry's most knowledgeable threat hunters, researchers, analysts, engineers and data scientists, working in dedicated threat research labs all around the world. FortiGuard Labs continuously monitors the global attack surface using millions of network sensors and hundreds of intelligence-sharing partners. It analyzes and processes this information using artificial intelligence (AI) and other innovative technologies to mine that data for new threats. These efforts result in timely, actionable threat intelligence in the form of Fortinet security product updates, proactive threat research that helps our customers better understand the threats and threat actors they face, and by providing specialized consulting services to help our customers identify and strengthen their security exposures. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FORTINET®

www.fortinet.com

November 10, 2020 8:16 AM

D:\Fortinet\White Paper\Teal White Paper\TEAL - Cyberthreat Predictions\wp-FA-cyber-threat-predictions-for-2021-11102020

831850-0-0-EN