2021 Threat Predictions Report

By McAfee on Jan 13, 2021

The Year 2020 brought a historic pandemic and bad actors leveraging COVID-19-themed threats to test our security operations and our unprecedented shift to a remote work life. As we enter 2021, these concerns are still at the forefront, but we are also looking ahead to other cyber threats likely to confront us in the months and years ahead.

The December 2020 revelations around the SUNBURST campaigns exploiting the SolarWinds Orion platform have revealed a new attack vector – the supply chain – that will continue to be exploited.

The ever-increasing use of connected devices, apps and web services in our homes will also make us more susceptible to digital home break-ins. This threat is compounded by many individuals continuing to work from home, meaning this threat not only impacts the consumer and their families, but enterprises as well.

Attacks on cloud platforms and users will evolve into a highly polarized state where they are either “mechanized and widespread” or “sophisticated and precisely handcrafted”.

Mobile users will need to beware of phishing or smishing messages aimed at exploiting and defrauding them through mobile payment services.

The use of QR codes has notably accelerated during the pandemic, raising the specter of a new generation of social engineering techniques that seek to exploit consumers and gain access to their personal data.

Finally, the most sophisticated threat actors will increasingly use social networks to target high value individuals working in sensitive industry sectors and roles.

A new year offers hope and opportunities for consumers and enterprises, but also more cybersecurity challenges. I hope you find these helpful in planning your 2021 security strategies.

–Raj Samani, Chief Scientist and McAfee Fellow, Advanced Threat Research

Twitter @Raj_Samani

2021 Predictions

1. Supply Chain Backdoor Techniques to Proliferate

The revelations around the SolarWinds-SUNBURST espionage campaign will spark a proliferation in copycat supply chain attacks of this kind.

On December 13, 2020, the cybersecurity industry learned nation-state threat actors had compromised SolarWinds's Orion IT monitoring and management software and used it to distribute a malicious software backdoor called SUNBURST to dozens of that company's customers, including several high-profile U.S. government agencies.

This SolarWinds-SUNBURST campaign is the first major supply chain attack of its kind and has been referred to by many as the "Cyber Pearl Harbor" that U.S. cybersecurity experts have been predicting for a decade and a half.

The campaign also represents a shift in tactics where nation state threat actors have employed a new weapon for cyber-espionage. Just as the use of nuclear weapons at the end of WWII changed military strategy for the next 75 years, the use of a supply chain attack has changed the way we need to consider defense against cyber-attacks.

This supply chain attack operated at the scale of a worm such as WannaCry in 2017, combined with the precision and lethality of the 2014 Sony Pictures or 2015 U.S. government Office of Personnel Management (OPM) attacks.

Within hours of its discovery, the magnitude of the campaign became frighteningly clear to organizations responsible for U.S. national security, economic competitiveness, and even consumer privacy and security.

It enables U.S. adversaries to steal all manners of information, from inter-governmental communications to national secrets. Attackers can, in turn, leverage this information to influence or impact U.S. policy through malicious leaks. Every breached agency may have different secondary cyber backdoors planted, meaning that there is no single recipe to evict the intrusion across the federal government.

While some may argue that government agencies are legitimate targets for nation-state spy craft, the campaign also impacted private companies. Unlike government networks which store classified information on isolated networks, private organizations often have critical intellectual property on networks with access to the internet. Exactly what intellectual property or private data on employees has been stolen will be difficult to determine, and the full extent of the theft may never be known.

This type of attack also poses a threat to individuals and their families given that in today's highly interconnected homes, a breach of consumer electronics companies can result in attackers using their access to smart appliances such as TVs, virtual assistants, and smart phones to steal their information or act as a gateway to attack businesses while users are working remotely from home.

What makes this type of attack so dangerous is that it uses trusted software to bypass cyber defenses, infiltrate victim organizations with the backdoor and allow the attacker to take any number of secondary steps. This could involve stealing data, destroying data, holding critical systems for ransom, orchestrating system malfunctions that result in kinetic damage, or simply implanting additional malicious content throughout the organization to stay in control even after the initial threat appears to have passed.

McAfee believes the discovery of the SolarWinds-SUNBURST campaign will expose attack techniques that other malicious actors around the world will seek to duplicate in 2021 and beyond.

2. Hacking the Home to Hack the Office

By Suhail Ansari, Dattatraya Kulkarni and Steve Povolny

The increasingly dense overlay of numerous connected devices, apps and web services used in our professional and private lives will grow the connected home's attack surface to the point that it raises significant new risks for individuals and their employers.

While the threat to connected homes is not new, what is new is the emergence of increased functionality in both home and business devices, and the fact that these devices connect to each other more than ever before. Compounding this is the increase in remote work – meaning many of us are using these connected devices more than ever.

of connected home devices globally and a 60% increase in the U.S. Over 70% of the traffic from these devices originated from smart phones, laptops, other PCs and TVs, and over 29% originated from IoT devices such as streaming devices, gaming consoles, wearables, and smart lights.

McAfee saw cybercriminals increase their focus on the home attack surface with a surge in various phishing message schemes across communications channels. The number of malicious phishing links McAfee blocked grew over 21% from March to November, at an average of over 400 links per home.

This increase is significant and suggests a flood of phishing messages with malicious links entered home networks through devices with weaker security measures.

Millions of individual employees have become responsible for their employer's IT security in a home office filled with "soft" targets, unprotected devices from the kitchen, to the family room, to the bedroom. Many of these home devices are "orphaned" in that their manufacturers fail to properly support them with security updates addressing new threats or vulnerabilities.

This contrasts with a corporate office environment filled with devices "hardened" by enterprise-grade security measures. We now work with consumer-grade networking equipment configured by "us" and lacking the central management, regular software updates and security monitoring of the enterprise.

Because of this, we believe cybercriminals will advance the home as an attack surface for campaigns targeting not only our families but also corporations. The hackers will take advantage of the home's lack of regular firmware updates, lack of security mitigation features, weak privacy policies, vulnerability exploits, and user susceptibility to social engineering.

By compromising the home environment, these malicious actors will launch a variety of attacks on corporate as well as consumer devices in 2021.

3. Attacks on Cloud Platforms Become Highly Mechanized and Handcrafted

By Sandeep Chandana

Attacks on cloud platforms will evolve into a highly polarized state where they are either "mechanized and widespread" or "targeted and precisely handcrafted".

The COVID-19 pandemic has also hastened the pace of the corporate IT transition to the cloud, accelerating the potential for new corporate cloud-related attack schemes. With increased cloud adoption and the large number of enterprises working from home, not only is there a growing number of cloud users but also a lot more data both in motion and being transacted.

McAfee cloud usage data from more than 30 million McAfee MVISION Cloud users worldwide shows a 50% increase overall in enterprise cloud use across all industries the first four months of 2020. Our analysis showed an increase across all cloud categories, usage of collaboration services such as Microsoft O365 by 123%, increase in use of business services such as Salesforce by 61% and the largest growth in collaboration services such as Cisco Webex (600%), Zoom (+350%), Microsoft Teams (+300%), and Slack (+200%). From January to April 2020, corporate cloud traffic from unmanaged devices increased 100% across all verticals.

During the same period, McAfee witnessed a surge in attacks on cloud accounts, an estimated 630% increase overall, with variations in the sectors that were targeted. Transportation led vertical industries with a 1,350% increase in cloud attacks, followed by education (+1,114%), government (+773%), manufacturing (+679%), financial services (+571%) and energy and utilities (+472%).

The increasing proportion of unmanaged devices accessing the enterprise cloud has effectively made home networks an extension of the enterprise infrastructure. Cybercriminals will develop new, highly mechanized, widespread attacks for better efficacy against thousands of heterogenous home networks.

password for multiple or all accounts according to a 2019 security survey conducted by Google. Where an attacker would traditionally need to manually encode first and last name combinations to find valid usernames, a learning algorithm could be used to predict O365 username patterns.

Additionally, cybercriminals could use AI and ML to bypass traditional network filtering technologies deployed to protect cloud instances. Instead of launching a classic brute force attack from compromised IPs until the IPs are blocked, resource optimization algorithms will be used to make sure the compromised IPs launch attacks against multiple services and sectors, to maximize the lifespan of compromised IPs used for the attacks. Distributed algorithms and reinforcement learning will be leveraged to identify attack plans primarily focused on avoiding account lockouts.

McAfee also predicts that, as enterprise cloud security postures mature, attackers will be forced to handcraft highly targeted exploits for specific enterprises, users and applications.

The recent Capital One breach was an example of an advanced attack of this kind. The attack was thoroughly cloud-native. It was sophisticated and intricate in that a number of vulnerabilities and misconfigurations across cloud applications (and infrastructure) were exploited and chained. It was not a matter of chance that the hackers were successful, as the attack was very well hand-crafted.

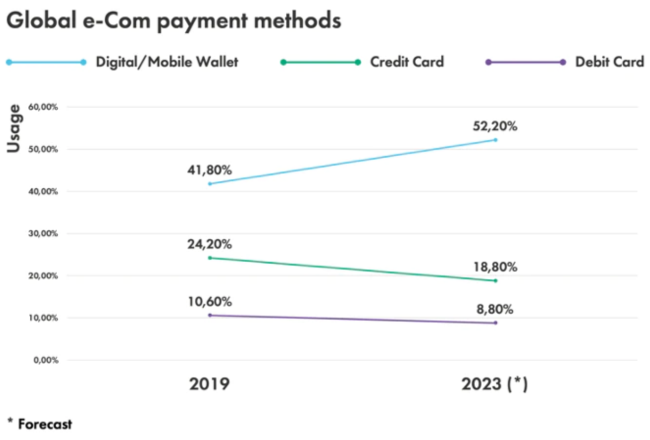
We believe attackers will start leveraging threat surfaces across devices, networks and the cloud in these ways in the months and years ahead.

4. New Mobile Payment Scams

By Suhail Ansari and Dattatraya Kulkarni

As users become more and more reliant on mobile payments, cybercriminals will increasingly seek to exploit and defraud users with scam SMS phishing or smishing messages containing malicious payment URLs.

Mobile payments have become more and more popular as a convenient mechanism to conduct transactions. A Worldpay Global Payments Report for 2020 estimated that 41% of payments today are on mobile devices, and this number looks to increase at the expense of traditional credit and debit cards by 2023. An October 2020 study by Allied Market Research found that the global mobile payment market size was valued at $1.48 trillion in 2019, and is projected to reach $12.06 trillion by 2027, growing at a compound annual growth rate of 30.1% from 2020 to 2027.



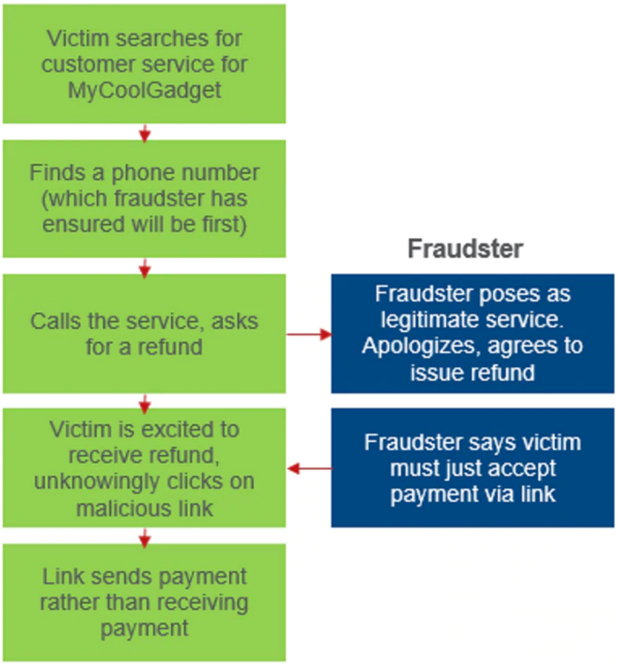
Source: Worldpay Global Payments Report 2020

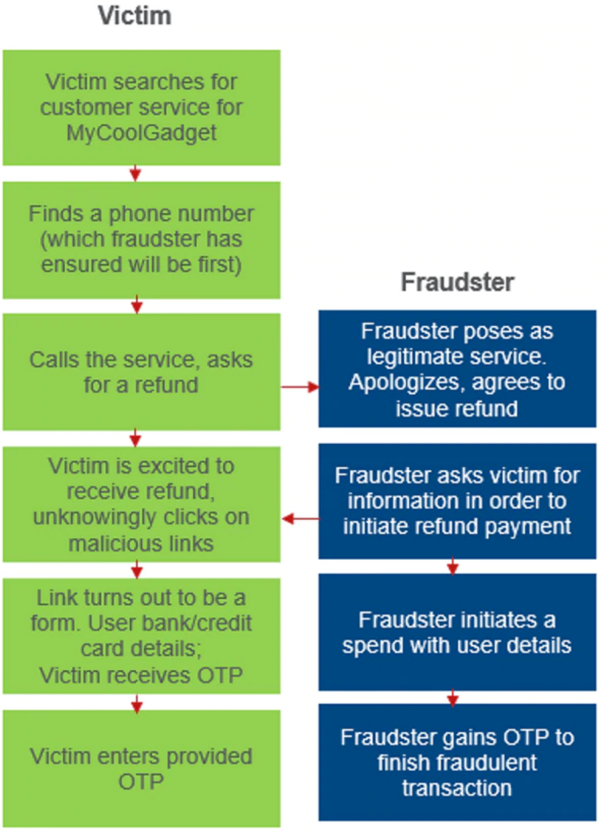
Additionally, the COVID-19 pandemic has driven the adoption of mobile payment methods higher as consumers have sought to avoid contact-based payments such as cash or physical credit cards.

But fraudsters have followed the money to mobile, pivoting from PC browsers and credit cards to mobile payments. According to research by RSA's Fraud and Risk Intelligence team, 72% of cyber fraud activity involved the mobile channel in the fourth quarter of

McAfee predicts there will be an increase in “receive”-based mobile payment exploits, where a user receives a phishing email, direct message or smishing message telling him that he can receive a payment, transaction refund or cash prize by clicking on a malicious payment URL. Instead of receiving a payment, however, the user has been conned into sending a payment from his account.

This could take shape in schemes where fraudsters set up a fake call center using a product return and servicing scam, where the actors send a link via email or SMS, offering a refund via a mobile payment app, but the user is unaware that they are agreeing to pay versus receiving a refund. The figures below show the fraudulent schemes in action.


Victim searches for customer service for MyCoolGadget
Finds a phone number (which fraudster has ensured will be first)
Calls the service, asks for a refund
Victim is excited to receive refund, unknowingly clicks on malicious link
Link sends payment rather than receiving payment
Fraudster
Fraudster poses as legitimate service. Apologizes, agrees to issue refund
Fraudster says victim must just accept payment via link


Victim
Victim searches for customer service for MyCoolGadget
Finds a phone number (which fraudster has ensured will be first)
Calls the service, asks for a refund
Victim is excited to receive refund, unknowingly clicks on malicious links
Link turns out to be a form. User bank/credit card details; Victim receives OTP
Victim enters provided OTP
Fraudster
Fraudster poses as legitimate service. Apologizes, agrees to issue refund
Fraudster asks victim for information in order to initiate refund payment
Fraudster initiates a spend with user details
Fraudster gains OTP to finish fraudulent transaction

Mobile wallets are making efforts to make it easier for users to understand whether they are paying or receiving. Unfortunately, as the payment methods proliferate, fraudsters succeed in finding victims who either cannot distinguish credit from debit or can be prompted into quick action by smart social engineering.

that the caller ID is not masked by fraudsters, but they do not prevent a fraudster from registering an entity that has a name close to the genuine provider of service.

In the same way that mobile apps have simplified the ability to conduct transactions, McAfee predicts the technology is making it easier to take advantage of the convenience for fraudulent purposes.

5. Qshing: QR Code Abuse in the Age of COVID

By Suhail Ansari and Dattatraya Kulkarni

Cybercriminals will seek new and ever cleverer ways to use social engineering and QR Code practices to gain access to consumer victims' personal data.

The global pandemic has created the need for all of us to operate and transact in all areas of our lives in a "contactless" way. Accordingly, it should come as no surprise that QR codes have emerged as a convenient input mechanism to make mobile transactions more efficient.

QR code usage has proliferated into many areas, including payments, product marketing, packaging, restaurants, retail, and recreation just to name a few. QR codes are helping limit direct contact between businesses and consumers in every setting from restaurants to personal care salons, to fitness studios. They allow them to easily scan the code, shop for services or items offered, and easily purchase them.

A September 2020 survey by MobileIron found that 86% of respondents scanned a QR code over the course of the previous year and over half (54%) reported an increase in the use of such codes since the pandemic began. Respondents felt most secure using QR codes at restaurants or bars (46%) and retailers (38%). Two-thirds (67%) believe that the technology makes life easier in a touchless world and over half (58%) wish to see it used more broadly in the future.

In just the area of discount coupons, an estimated 1.7 billion coupons using QR codes were scanned globally in 2017, and that number is expected to increase by a factor of three to 5.3 billion by 2022. In just four years, from 2014 to 2018, the use of QR codes on consumer product packaging in Korea and Japan increased by 83%. The use of QR codes in such "smart" packaging is increasing at an annual rate of 8% globally.

In India, the government's Unique Identification Authority of India (UIDAI) uses QR codes in association with Aadhaar, India's unique ID number, to enable readers to download citizens' demographic information as well as their photographs.

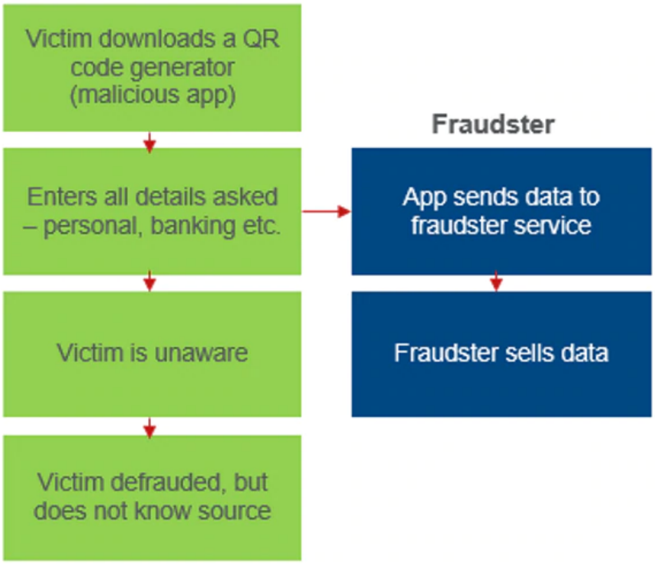
However, the technicalities of QR codes are something of a mystery to most users, and that makes them potentially dangerous if cybercriminals seek to exploit them to target victims.

The MobileIron report found that whereas 69% of respondents believe they can distinguish a malicious URL based on its familiar text-based format, only 37% believe they can distinguish a malicious QR code using its unique dot pattern format. Given that QR codes are designed precisely to hide the text of the URL, users find it difficult to identify and even suspect malicious QR codes.

Almost two-thirds (61%) of respondents know that QR codes can open a URL and almost half (49%) know that a QR code can download an application. But fewer than one-third (31%) realize that a QR code can make a payment, cause a user to follow someone on social media (22%), or start a phone call (21%). A quarter of respondents admit scanning a QR code that did something unexpected (such as take them to a suspicious website), and 16% admitted that they were unsure if a QR code actually did what it was intended to do.

It is therefore no surprise that QR codes have been used in phishing schemes to avoid anti-phishing solutions' attempts to identify malicious URLs within email messages. They can also be used on webpages or social media.

In such schemes, victims scan fraudulent QRs and find themselves taken to malicious websites where they are asked to provide login, personal info, usernames and passwords, and payment information, which criminals then steal. The sites could also be used to simply download malicious programs onto a user's device.


Victim downloads a QR code generator (malicious app)
Enters all details asked – personal, banking etc.
Victim is unaware
Victim defrauded, but does not know source
Fraudster
App sends data to fraudster service
Fraudster sells data

McAfee predicts that hackers will increasingly use these QR code schemes and broaden them using social engineering techniques. For instance, knowing that business owners are looking to download QR code generator apps, bad actors will entice consumers into downloading malicious QR code generator apps that pretend to do the same. In the process of generating the QR code (or even pretending to be generating the correct QR code), the malicious apps will steal the victim's sensitive data, which scammers could then use for a variety of fraudulent purposes.

Although the QR codes themselves are a secure and convenient mechanism, we expect them to be misused by bad actors in 2021 and beyond.

6. Social Networks as Workplace Attack Vectors

By Raj Samani

McAfee predicts that sophisticated cyber adversaries will increasingly target, engage and compromise corporate victims using social networks as an attack vector.

Cyber adversaries have traditionally relied heavily on phishing emails as an attack vector for compromising organizations through individual employees. However, as organizations have implemented spam detection, data loss prevention (DLP) and other solutions to prevent phishing attempts on corporate email accounts, more sophisticated adversaries are pivoting to target employees through social networking platforms to which these increasingly effective defenses cannot be applied.

McAfee has observed such threat actors increasingly using the messaging features of LinkedIn, What's App, Facebook and Twitter to engage, develop relationships with and then compromise corporate employees. Through these victims, adversaries compromise the broader enterprises that employ them. McAfee predicts that such actors will seek to broaden the use of this attack vector in 2021 and beyond for a variety of reasons.

Malicious actors have used the social network platforms in broad scoped schemes to perpetrate relatively low-level criminal scams. However, prominent actors such as APT34, Charming Kitten, and Threat Group-2889 (among others) have been identified using these platforms for higher-value, more targeted campaigns on the strength of the medium's capacity for enabling customized content for specific types of victims.

Operation North Star demonstrates a state-of-the-art attack of this kind. Discovered and exposed by McAfee in August 2020, the campaign showed how lax social media privacy controls, ease of development and use of fake LinkedIn user accounts and job descriptions could be used to lure and attack defense sector employees.

target high value employees with a deeper level of engagement.

Additionally, individual employees engage with social networks in a capacity that straddles both their professional and personal lives. While enterprises assert security controls over corporate-issued devices and place restrictions on how consumer devices access corporate IT assets, user activity on social network platforms is not monitored or controlled in the same way. As mentioned, LinkedIn and Twitter direct messaging will not be the only vectors of concern for the corporate security operations center (SOC).

While it is unlikely that email will ever be replaced as an attack vector, McAfee foresees this social network platform vector becoming more common in 2021 and beyond, particularly among the most advanced actors.

About the Author

McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. Take a look at our latest blogs.

Read more posts from McAfee ›

‹ Previous Article Next Article ›

Categories: McAfee Labs