Advanced Threat predictions for 2021

By GReAT

Trying to make predictions about the future is a tricky business. However, while we don't have a crystal ball that can reveal the future, we can try to make educated guesses using the trends that we have observed over the last 12 months to identify areas that attackers are likely to seek to exploit in the near future.

Let's start by reflecting on our predictions for 2020.

- **The next level of false flag attacks**
  This year, we haven't seen anything as dramatic as the forging of a malicious module to make it look like the work of another threat actor, as was the case with Olympic Destroyer. However, the use of false flags has undoubtedly become an established method used by APT groups to try to deflect attention away from their activities. Notable examples this year include the campaigns of MontysThree and DeathStalker. Interestingly, in the DeathStalker case, the actor incorporated certificate metadata from the infamous Sofacy in their infrastructure, trading covertness for the chance of having their operation falsely attributed.
- **From ransomware to targeted ransomware**
  Last year, we highlighted the shift towards targeted ransomware and predicted that attackers would use more aggressive methods to extort money from their victims. This year, hardly a week has gone by without news of an attempt to extort money from large organizations, including recent attacks on a number of US hospitals. We've also seen the emergence of 'brokers' who offer to negotiate with the attackers, to try to reduce the cost of the ransom fee. Some attackers seem to apply greater pressure by stealing data before encrypting it and threatening to publish it; and in a recent incident, affecting a large psychotherapy practice, the attackers posted sensitive data of patients.
- **New online banking and payments attack vectors**
  We haven't seen any dramatic attacks on payment systems this year. Nevertheless, financial institutions continue to be targeted by specialist cybercrime groups such as FIN7, CobaltGroup, Silence and Magecart, as well as APT threat actors such as Lazarus.
- **More infrastructure attacks and attacks against non-PC targets**
  APT threat actors have not confined their activities to Windows, as illustrated by the extension of Lazarus's MATA framework, the development of Turla's Penquin_x64 backdoor and the targeting of European supercomputing centers in May. We also saw the use of multiplatform, multi-architecture tools such as Termite and Earthworm in operation TunnelSnake. These tools are capable of creating tunnels, transferring data and spawning remote shells on the targeted machines, supporting x86, x64, MIPS(ES), SH-4, PowerPC, SPARC and M68k. On top of this, we also discovered the framework we dubbed MosaicRegressor, which includes a compromised UEFI firmware image designed to drop malware onto infected computers.
- **Increased attacks in regions that lie along the trade routes between Asia and Europe**
  In 2020, we observed several APT threat actors target countries that had previously drawn less attention. We saw various malware used by Chinese-speaking actors used against government targets in Kuwait, Ethiopia, Algeria,

Myanmar and the Middle East. We also observed StrongPity deploying a new, improved version of their main implant called StrongPity4. In 2020 we found victims infected with StrongPity4 outside Turkey, located in the Middle East.

- **Increasing sophistication of attack methods**
  In addition to the UEFI malware mentioned above, we have also seen the use of legitimate cloud services (YouTube, Google Docs, Dropbox, Firebase) as part of the attack infrastructure (either geo-fencing attacks or hosting malware and used for C2 communications).
- **A further change of focus towards mobile attacks**
  This is apparent from the reports we have published this year. From year to year we have seen more and more APT actors develop tools to target mobile devices. Threat actors this year included OceanLotus, the threat actor behind TwoSail Junk, as well as Transparent Tribe, OrigamiElephant and many others.
- **The abuse of personal information: from deep fakes to DNA leaks**
  Leaked/stolen personal information is being used more than ever before in up-close and personal attacks. Threat actors are less afraid than ever to engage in active ongoing communications with their victims, as part of their spear-phishing operations, in their efforts to compromise target systems. We have seen this, for example, in Lazarus's ThreatNeedle activities and in DeathStalker's efforts to pressure victims into enabling macros. Criminals have used AI software to mimic the voice of a senior executive, tricking a manager into transferring more than £240,000 into a bank account controlled by fraudsters; and governments and law enforcement agencies have used facial recognition software for surveillance.

Turning our attention to the future, these are some of the developments that we think will take center stage in the year ahead, based on the trends we have observed this year.

APT threat actors will buy initial network access from cybercriminals

In the last year, we have observed many targeted ransomware attacks using generic malware, such as Trickbot, to gain a foothold in target networks. We have also observed connections between targeted ransomware attacks and well-established underground networks like Genesis that typically trade in stolen credentials. We believe APT actors will start using the same method to compromise their targets. Organizations should pay increased attention to generic malware and perform basic incident response activities on each compromised computer to ensure generic malware has not been used deploy sophisticated threats.

More countries using legal indictments as part of their cyberstrategy

Some years ago we predicted that governments would resort to "naming and shaming", to draw attention to the activities of hostile APT groups. We have seen several cases of this over the last 12 months. We think that US Cyber Command's "persistent engagement" strategy will begin to bear fruit in the coming year and lead other states to follow suit, not least as "tit for tat" retaliation to US indictments. Persistent engagement involves publicly releasing reports about adversary tools and activities. US Cyber Command has argued that warfare in cyberspace is of a

fundamentally different nature, and requires full-time engagement with adversaries to disrupt their operations. One of the ways they do so is by providing indicators that the threat intelligence community can use to bootstrap new investigations – in a sense, it is a way of orienting private research through intelligence declassification.

Tools "burned" in this way become harder to use for the attackers, and can undermine past campaigns that might otherwise have stayed under the radar. Faced with this new threat, adversaries planning attacks must factor in additional costs (the heightened possibility of losing tools or these tools being exposed) in their risk/gain calculus.

Exposing toolsets of APT groups is nothing new: successive leaks by Shadow Brokers provide a striking example. However, it is the first time it has been done in an official capacity through state agencies. While quantifying the effects of deterrence is impossible, especially without access to diplomatic channels where such matters are discussed, we believe that more countries will follow this strategy in 2021. First, states traditionally aligned with the US may start replicating the process, and then, later on, the targets of such disclosures could follow suit as a form of retaliation.

More Silicon Valley companies will take action against zero-day brokers

Until recently, zero-day brokers have traded exploits for well-known commercial products; and big companies such as Microsoft, Google, Facebook and others have seemingly paid little attention to the trade. However, in the last year or so, there have been high-profile cases where accounts were allegedly compromised using WhatsApp vulnerabilities – including Jeff Bezos and Jamal Khashoggi. In October 2019, WhatsApp filed a lawsuit accusing Israel-based NSO Group of having exploited a vulnerability in its software; and that the technology sold by NSO was used to target more than 1,400 of its customers in 20 different countries, including human rights activists, journalists and others. A US judge subsequently ruled that the lawsuit could proceed. The outcome of the case could have far-reaching consequences, not least of which could be to lead other firms to take legal action against companies that deal in zero-day exploits. We think that mounting public pressure, and the risk of reputation damage, may lead other companies to follow WhatsApp's lead and take action against zero-day brokers, to demonstrate to their customers that they are seeking to protect them.

Increased targeting of network appliances

With the trend towards overall improvement of organizational security, we think that actors will focus more on exploiting vulnerabilities in network appliances such as VPN gateways. We're already starting to see this happen – see here, here and here for further details. This goes hand-in-hand with the shift towards working from home, requiring more companies to rely on a VPN setup in their business. The increased focus on remote working, and reliance on VPNs, opens up another potential attack vector: the harvesting of user credentials through real-world social engineering approaches such as "vishing" to obtain access to corporate VPNs. In some cases, this might allow the attacker to even accomplish their espionage goals without deploying malware in the victim's environment.

The emergence of 5G vulnerabilities

5G has attracted a lot of attention this year, with the US exerting a lot of pressure on friendly states to discourage them from buying Huawei products. In many countries, there were also numerous scare stories about possible health risks, etc. This focus on 5G security means that researchers, both public and private, are definitely looking at the products of Huawei and others, for signs of implementation problems, crypto flaws and even backdoors. Any such flaws will certainly receive massive media attention. As usage of 5G increases, and more devices become dependent on the connectivity it provides, attackers will have a greater incentive to look for vulnerabilities that they can exploit.

Demanding money "with menaces"

We have seen several changes and refinements in the tactics used by ransomware gangs over the years. Most notably, attacks have evolved from random, speculative attacks distributed to a large number of potential victims, to highly targeted attacks that demand a considerably greater payout from a single victim at a time. The victims are carefully selected, based on their ability to pay, their reliance on the data encrypted and the wider impact an attack will have. And no sector is considered off limits, notwithstanding the promises ransomware gangs made not to target hospitals. The delivery method is also customized to fit the targeted organization, as we have seen with attacks on medical centers and hospitals throughout the year.

We have also seen ransomware gangs seeking to obtain greater leverage by threatening to publish stolen data if a company fails to pay the ransom demanded by the attackers. This trend is likely to develop further as ransomware gangs seek to maximize their return on investment.

The ransomware problem has become so prevalent that the OFAC (Office of Foreign Assets Control) released instructions for victims and clarified that paying ransoms could constitute a breach of international sanctions. We interpret this announcement as the beginning of a wider crackdown on the cybercrime world by US authorities.

This year, the Maze and Sodinokibi gangs both pioneered an "affiliate" model involving collaboration between groups. Nevertheless, the ransomware eco-system remains very diverse. It's possible that in the future we will see a concentration of major ransomware players who will start to focus their activities and obtain APT-like capabilities. However, for some time to come, smaller gangs will continue to adopt the established approach that relies on piggybacking botnets and sourcing third-party ransomware.

More disruptive attacks

More and more aspects of our lives are becoming dependent on technology and connectivity to the internet. As a result, we present a much wider attack surface than ever before. It's likely, therefore, that we will see more disruptive attacks in the future. On the one hand, this disruption could be the result of a directed, orchestrated attack, designed to affect critical infrastructure. On the other hand, it could be collateral damage that occurs as a side-effect of a large-volume ransomware attack targeting organizations that we use in our day-to-day lives, such as educational institutions, supermarkets, postal services and public transportation.

Attackers will continue to exploit the COVID-19 pandemic

The world has been turned upside down by COVID-19, which has impacted nearly every aspect of our lives this year. Attackers of all kinds were quick to seize the opportunity to exploit the keen interest in this topic, including APT threat actors. As we have noted before, this did not mark a change in TTPs, but simply a persistent topic of interest that they could use as a social engineering lure. The pandemic will continue to affect our lives for some time to come; and threat actors will continue to exploit this to gain a foothold in target systems. During the last six months, there have been reports of APT groups targeting COVID-19 research centers. The UK National Cyber Security Centre (NCSC) stated that APT29 (aka the Dukes and Cozy Bear) targeted COVID-19 vaccine development. This will remain a target of strategic interest to them for as long as the pandemic lasts.