Kaspersky Security Bulletin

Advanced threat predictions for 2020

kaspersky

CONTENTS

kaspersky

ADVANCED THREAT PREDICTIONS FOR 2020

Nothing is more difficult than making predictions. Rather than trying to gaze into a crystal ball, we will be making educated guesses based on what has happened during the last 12 months, to see where we can see trends that might be exploited in the near future.

This is what we think might happen in the coming months, based on the knowledge of experts in this field and our observation of APT attacks – since APT threat actors have historically been the center of innovation.

The next level of false flag attacks

We should consider how actors continually use commodity malware, scripts, publicly available security tools or administrator software during their attacks and for lateral movement, making attribution increasingly difficult

The use of false flags has become an important element in the playbook of several APT groups. In the past, this has generally involved trying to deflect attention away from those responsible for the attack – for instance, the usage of Russian words in Lazarus group malware, or Romanian words by WildNeutron. In one notable case – the Olympic Destroyer attack – the Hades APT group sought to go further than just clouding the waters of attribution by forging elements of the attack to make it seem like the work of a different threat actor. We believe that this will develop further, with threat actors seeking not only to avoid attribution but to actively lay the blame on someone else.

For instance, this could include the usage of established backdoors by other unrelated APT actors, the theft and re-use of code (the recently published case of Turla reusing code from an unknown Iranian group, outlined by the UK NCSC and NSA comes to mind) or deliberately leaking source code so that other groups adopt it and muddy the waters further.

On top of all that, we should consider how actors continually use commodity malware, scripts, publicly available security tools or administrator software during their attacks and for lateral movement, making attribution increasingly difficult. Mixing a couple of false flags into this equation, where security researchers are hungry for any small clue, might be enough to divert authorship to someone else.

kaspersky

Ransomware is, unfortunately, the most effective tool for extracting a financial profit from the victims.

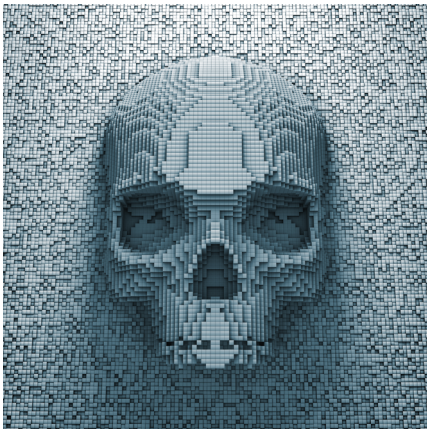
From ransomware to targeted ransomware

In the last two years we've seen a decline in numbers of all-purpose widespread ransomware attacks as cybercriminals have become more targeted in their use of this type of malware – focusing on organizations that are likely to make substantial payments in order to recover their data. We are calling this technique 'targeted ransomware'. Throughout the year, we recorded several cases where attackers used targeted ransomware, and we think that a likely future development will be more aggressive attempts to extort money. A potential twist might be that, instead of making files unrecoverable, threat actors will threaten to publish data that they have stolen from the victim company.

In addition to targeted ransomware, it is inevitable that the cybercriminals will also attempt to diversify their attacks to include other types of devices besides PCs or servers. For instance, ransomware in consumer products, such as smart TVs, smart watches, smart cars/houses/cities. As more devices become connected to the internet, cybercriminals will also be looking for ways to monetize their access to these devices. Ransomware is, unfortunately, the most effective tool for extracting a financial profit from the victims.

New online banking and payments attack vectors

A new potential attack vector for cybercriminals could open up with the new banking regulations that have recently come into full effect across the EU. The PSD2 (Payments Services Directive) lays down regulatory requirements for companies that provide payment services, including the use of personal data by new fintech companies that are not part of the established banking community. Security of online, including mobile, payments is a key aspect of the legislation. Nevertheless, as banks will be required to open their infrastructure and data to third parties who wish to provide services to bank customers, it is likely that attackers will seek to abuse these new mechanisms with new fraudulent schemes.



More infrastructure attacks and attacks against non-PC targets

Determined threat actors have, for some time, been extending their toolsets beyond Windows, and even beyond PC systems: VPNFilter and Slingshot, for example, targeted networking hardware. The benefit to an attacker, of course, is that once they have compromised such devices, it gives them flexibility. They could opt for a massive botnet-style compromise and use that network in the future for different goals, or they might approach selected targets for more clandestine attacks. In our threat predictions for 2019, we considered the possibility of 'malware-less' attacks, where opening a VPN tunnel to mirror or redirect traffic might provide all the necessary information to an attacker. In June, it was revealed that hackers had infiltrated the networks of at least 10 cellular telcos around the world, and had remained hidden for years. In some cases, it seems they had been able to deploy their own VPN services on telco infrastructure. The convergence of real and cyber worlds brought about by the profusion of IoT devices offers growing opportunities for attackers; and it's evident that threat actors are aware of the potential. This year it was reported that unknown attackers stole 500MB of data from NASA's Jet Propulsion Laboratory using a Raspberry Pi. In December last year, the UK's Gatwick airport was brought to a standstill for fear of a possible collision after at least one drone was sighted above one of the runways. While it's unclear whether this was the result of a hobbyist drone owner or a determined DDoS attacker, the fact remains that part of the country's critical infrastructure was brought to a standstill because of the use of a drone. The number of such attacks will undoubtedly grow.

In recent years, we have seen a number of high-profile attacks on critical infrastructure facilities and these have typically been aligned to wider geo-political objectives. While most infections in industrial facilities continue to be from 'mainstream' malware, this fact itself highlights just how vulnerable these facilities can be. While targeted attacks on critical infrastructure facilities are unlikely ever to become a mainstream criminal activity, we do expect to see the number grow in the future. Geo-political conflicts are now played out in a world where the physical and cyber are increasingly converging; and, as we have observed before, such attacks offer governments a form of retaliation that lies between diplomacy and war.

"War is merely the continuation of politics by other means"

Increased attacks in regions that lie along the trade routes between Asia and Europe

Clausewitz's dictum, "War is merely the continuation of politics by other means", can be extended to include cyberconflict, with cyberattacks reflecting wider real-world tensions and conflicts. We have seen numerous examples. Consider, for example, accusations of Russian interference in US elections and fears about a possible reboot of this in the run-up to the 2020 elections. We've seen it in the 'naming-and-shaming' of alleged Chinese hackers in US indictments. The widespread use of mobile implants to surveil 'persons of interest' is another example.

There are several ways this could play out. They include a growth in political espionage as governments seek to secure their interests at home and abroad. This could mean monitoring the activities of 'undesirable' individuals or movements within the country, as well as those of potential opponents abroad. It is likely to extend also to technological espionage in situations of potential or real economic crisis and resulting instability. This could result in new attacks in regions that lie along trade routes between Asia and Europe, including Turkey, East and South Europe and East Africa.

It's quite possible that we will see changes to legislation and policy, as governments look to define more clearly what is and what isn't allowed. On the one hand, this could be used as a way to establish plausible deniability and thereby avoid sanctions if the finger of suspicion is pointed at one state by another. On the other hand, it could enable more aggressive use of technology, as several justice departments seem keen to open the door to different kinds of 'lawful interception' to collect evidence on computers. One likely response from criminal groups will be greater use of encryption and the Darknet to conceal their operations.

It could enable more aggressive use of technology, as several justice departments seem keen to open the door to different kinds of 'lawful interception' to collect evidence on computers

Increasing sophistication of attack methods

It is hard to know exactly how advanced the top-class attackers really are and what kind of resources they have in their pockets. Of course, every year we learn a bit more: for instance, a few years ago we observed an apparent endless supply of zero-days for resourceful attackers who were ready to pay for them. This year we observed several examples, but probably the most interesting is the one involving at least 14 exploits for iOS during the last two years, as exposed by Google in August.

The new isolation methods implemented for Microsoft Word and other software traditionally targeted in spear-phishing campaigns might have a significant impact in malware delivery methods, forcing less sophisticated actors to change the way they spread malware.

We believe it is likely that additional interception capabilities, similar to the Quantum insert attacks described a few years ago, are already being used; and hopefully we will be able to discover some of them.

It also seems likely that attackers will exfiltrate data with non-conventional methods, such as using signaling data or Wi-Fi/4G, especially when using physical implants (something we also believe is probably being overlooked). In a similar vein, we believe more attackers will use DoH (DNS over HTTPS) in the future to conceal their activities and make discovery more difficult. Finally, it is possible that during the coming months we will start discovering more UEFI malware and infections as our ability to see such systems is slowly improving.

Use of supply chains will continue to be one of the most difficult delivery methods to address. It is likely that attackers will continue to expand this method through manipulated software containers, for example, and abuse of packages and libraries.

A change of focus towards mobile attacks

During the last 10 years, an important transition has taken place: the main storage for our digital lives has moved from the PC to mobiles.

During the last 10 years, an important transition has taken place: the main storage for our digital lives has moved from the PC to mobiles. Some threat actors were quick to notice this and begin focusing on developing attack tools for mobiles. While we have constantly been predicting a huge increase in the number of attacks against mobiles, the observations from the field haven't always reflected this inferred evolution. However, the lack of observations of a phenomenon doesn't necessarily imply that it's not happening.

We have already discussed how an attacker abused at least 14 zero-day vulnerabilities in iOS to target certain minorities in Asia. We also saw recently how Facebook sued the Israeli company NSO for allegedly misusing its servers (to deploy malware to intercept user data). We also saw how Android zero-click, full persistence exploits are now more expensive (according to Zerodium's price list) than those for the iPhone.

All of this is telling us how much money attackers are investing in developing these technologies. It is clear to all of them how nearly everyone has a phone in his/her pocket and how valuable the information on those devices is. Every year we see new movements in this direction. We also see how complicated it might be for security researchers to obtain more technical details about attacks on such platforms, given the lack of visibility or accessibility.

There are no good reasons to think this will stop any time soon. However, due to the increased attention given to this subject by the security community, we believe the number of attacks being identified and analyzed in detail will also increase.

kaspersky

The abuse of personal information: from deep fakes to DNA leaks

We have previously discussed how data leaks help attackers to craft more convincing social engineering attacks. Not every adversary has a complete profile of potential victims to abuse, which makes the increasing amount of leaked data very valuable. This is also true for 'less targeted' attacks like the ransomware cases we have already discussed.

In a world where logged data continues to grow, we can see the danger in what could be considered especially sensitive leaks, for instance when it comes to biometric data. Also, widely discussed deepfakes are providing the technology to make such attacks a possibility, especially when combining this with less obvious attack vectors such as video and audio. We should not forget how this can be automated, and how AI can help with the profiling and creation of such scams.

Yes, all this sounds futuristic, but it is very similar to some of the techniques discussed for driving election advertisements through social media. This technology is already in use and it is just a matter of time before some attackers take advantage of it.

The future holds so many possibilities that there are likely to be things that are not included in our predictions. The extent and complexity of the environments in which attacks play out offer so many possibilities. In addition, no single threat research team has complete visibility of the operations of APT threat actors. We will continue to try and anticipate the activities of APT groups and understand the methods they employ, while providing insights into their campaigns and the impact they have.