KASPERSKY lab

Kaspersky Security Bulletin:

THREAT PREDICTIONS FOR 2019

Vicente Diaz

CONTENTS

There's nothing more difficult than predicting. So, instead of gazing into a crystal ball, the idea here is to make educated guesses based on what has happened recently and where we see a trend that might be exploited in the coming months. Asking the most intelligent people I know, and basing our scenario on APT attacks because they traditionally show the most innovation when it comes to breaking security, here are our main 'predictions' of what might happen in the next few months.

NO MORE BIG APTS

What? How is it possible that in a world where we discover more and more actors every day the first prediction seems to point in the opposite direction?

The reasoning behind this is that the security industry has consistently discovered highly sophisticated government-sponsored operations that took years of preparation. What seems to be a logical reaction to that situation from an attacker's perspective would be exploring new, even more sophisticated techniques that are much more difficult to discover and to attribute to specific actors.

Indeed, there are many different ways of doing this. The only requirement would be an understanding of the techniques used by the industry for attribution and for identifying similarities between different attacks and the artifacts used in them– something that doesn't seem to be a big secret. With sufficient resources, a simple solution for an attacker could be having different ongoing sets of activity that are very difficult to relate to the same actor or operation. Well-resourced attackers could start new innovative operations while keeping their old ones alive. Of course, there's still a good chance of the older operations being discovered, but discovering the new operations would pose a greater challenge.

Instead of creating more sophisticated campaigns, in some cases it appears to be more efficient for some very specific actors who have the capability to do so, to directly target infrastructure and companies where victims can be found, such as ISPs. Sometimes this can be accomplished through regulation, without the need for malware.

Some operations are simply externalized to different groups and companies that use different tools and techniques, making attribution extremely difficult. It's worth keeping in mind that in the case of government-sponsored operations this 'centrifugation' of resources and talent might affect the future of such campaigns.

Technical capabilities and tools are owned by the private industry in this scenario, and they are for sale for any customer that, in many cases, doesn´t fully understand the technical details and consequences behind them.

All this suggests that we're unlikely to discover new highly sophisticated operations – well-resourced attackers are more likely to simply shift to new paradigms.

NETWORKING HARDWARE AND IOT

It just seemed logical that at some point every actor would deploy capabilities and tools designed to target networking hardware. Campaigns like VPNFilter were a perfect example of how attackers have already started deploying their malware to create a multipurpose 'botnet'. In this particular case, even when the malware was extremely widespread, it took some time to detect the attack, which is worrisome considering what might happen in more targeted operations. Actually, this idea can go even further for well-resourced actors: why not directly target even more elemental infrastructure instead of just focusing on a target organization? We haven't reached that level of compromise (to our knowledge), but it was clear from past examples (like Regin) how tempting that level of control is for any attacker.

Vulnerabilities in networking hardware allow attackers to follow different directions. They might go 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 this second group we might consider 'malware-less' attacks, where opening a VPN tunnel to mirror or redirect traffic might provide all the necessary information to an attacker.

All these networking elements might also be part of the mighty IoT, where botnets keep growing at an apparently unstoppable pace. These botnets could be incredibly powerful in the wrong hands when it comes to disrupting critical infrastructure, for instance. This can be abused by well-resourced actors, possibly using a cover group, or in some kind of terror attack.

One example of how these versatile botnets can be used, other than for disruptive attacks, is in short-range frequency hopping for malicious communications, avoiding monitoring tools by bypassing conventional exfiltration channels.

Even though this seems to be a recurrent warning year after year, we should never underestimate IoT botnets – they keep growing stronger.

PUBLIC RETALIATION

One of the biggest questions in terms of diplomacy and geopolitics was how to deal with an active cyberattack. The answer is not simple and depends heavily on how bad and blatant the attack was, among many other considerations. However, it seems that after hacks like that on the Democratic National Committee, things became more serious.

Investigations into recent high-profile attacks, such as the Sony Entertainment Network hacks or the attack on the DNC, culminated in a list of suspects being indicted. That results not only in people facing trial but also a public show of who was behind the attack. This can be used to create a wave of opinion that might be part of an argument for more serious diplomatic consequences.

Actually we have seen Russia suffering such consequences as a result of their alleged interference in democratic processes. This might make others rethink future operations of this kind.

However, the fear of something like that happening, or the thought that it might already have happened, was the attackers' biggest achievement. They can now exploit such fear, uncertainty and doubt in different, more subtle ways – something we saw in notable operations, including that of the Shadowbrokers. We expect more to come.

What will we see in the future? The propaganda waters were probably just being tested by past operations. We believe this has just started and it will be abused in a variety of ways, for instance, in false flag incidents like we saw with Olympic Destroyer, where it's still not clear what the final objective was and how it might have played out.

EMERGENCE OF NEWCOMERS

Simplifying somewhat, the APT world seems to be breaking into two groups: the traditional well-resourced most advanced actors (that we predict will vanish) and a group of energetic newcomers who want to get in on the game.

The thing is that the entry barrier has never been so low, with hundreds of very effective tools, re-engineered leaked exploits and frameworks of all kinds publicly available for anyone to use. As an additional advantage, such tools make attribution nearly impossible and can be easily customized if necessary.

There are two regions in the world where such groups are becoming more prevalent: South East Asia and the Middle East. We have observed the rapid progression of groups suspected of being based in these regions, traditionally abusing social engineering for local targets, taking advantage of poorly protected victims and the lack of a security culture. However, as targets increase their defenses, attackers do the same with their offensive capabilities, allowing them to extend their operations to other regions as they improve the technical level of their tools. In this scenario of scripting-based tools we can also find emerging companies providing regional services who, despite OPSEC failures, keep improving their operations.

One interesting aspect worth considering from a more technical angle is how JavaScript post-exploitation tools might find a new lease of life in the short term, given the difficulty of limiting its functionality by an administrator (as opposed to PowerShell), its lack of system logs and its ability to run on older operating systems.

THE NEGATIVE RINGS

The year of Meltdown/Spectre/AMDFlaws and all the associated vulnerabilities (and those to come) made us rethink where the most dangerous malware actually lives. And even though we have seen almost nothing in the wild abusing vulnerabilities below Ring 0, the mere possibility is truly scary as it would be invisible to almost all the security mechanisms we have.

For instance, in the case of SMM there has at least been a publicly available PoC since 2015. SMM is a CPU feature that would effectively provide remote full access to a computer without even allowing Ring 0 processes to have access to its memory space. That makes us wonder whether the fact that we haven´t found any malware abusing this so far is simply because it is so difficult to detect. Abusing this feature seems to be too good an opportunity to ignore, so we are sure that several groups have been trying to exploit such mechanisms for years, maybe successfully.

We see a similar situation with virtualization/hypervisor malware, or with UEFI malware. We have seen PoCs for both, and HackingTeam even revealed a UEFI persistence module that's been available since at least 2014, but again no real ITW examples as yet.

Will we ever find these kinds of unicorns? Or haven't they been exploited yet? The latter possibility seems unlikely.

YOUR FAVORITE INFECTION VECTOR

In probably the least surprising prediction of this article we would like to say a few words about spear phishing. We believe that the most successful infection vector ever will become even more important in the nearest future. The key to its success remains its ability to spark the curiosity of the victim, and recent massive leaks of data from various social media platforms might help attackers improve this approach.

Data obtained from attacks on social media giants such as Facebook and Instagram, as well as LinkedIn and Twitter, is now available on the market for anyone to buy. In some cases, it is still unclear what kind of data was targeted by the attackers, but it might include private messages or even credentials. This is a treasure trove for social engineers, and could result in, for instance, some attacker using the stolen credentials of some close contact of yours to share something on social media that you already discussed privately, dramatically improving the chances of a successful attack.

This can be combined with traditional scouting techniques where attackers double-check the target to make sure the victim is the right one, minimizing the distribution of malware and its detection. In terms of attachments, it is fairly standard to make sure there is human interaction before firing off any malicious activity, thus avoiding automatic detection systems.

Indeed, there are several initiatives using machine learning to improve phishing's effectiveness. It's still unknown what the results would be in a real-life scenario, but what seems clear is that the combination of all these factors will keep spear phishing as a very effective infection vector, especially via social media in the months to come.

DESTRUCTIVE DESTROYER

Olympic destroyer was one of the most famous cases of potentially destructive malware during the past year, but many attackers are incorporating such capabilities in their campaigns on a regular basis. Destructive attacks have several advantages for attackers, especially in terms of creating a diversion and cleaning up any logs or evidence after the attack. Or simply as a nasty surprise for the victim.

Some of these destructive attacks have geostrategic objectives related to ongoing conflicts as we have seen in Ukraine, or with political interests like the attacks that affected several oil companies in Saudi Arabia. In some other cases they might be the result of hacktivism, or activity by a proxy group that's used by a more powerful entity that prefers to stay in the shadows.

Anyway, the key to all these attacks is that they are 'too good' not to use. In terms of retaliation for instance, governments might use them as a response ranged somewhere between a diplomatic answer and an act of war, and indeed some governments are experimenting with them. Most of these attacks are planned in advance, which involves an initial stage of reconnaissance and intrusion. We don´t know how many potential victims are already in this situation where everything is ready, just waiting for the trigger to be pulled, or what else the attackers have in their arsenal waiting for the order to attack.

ICS environments and critical infrastructure are especially vulnerable to such attacks, and even though industry and governments have put a lot of effort in over the last few years to improve the situation, things are far from ideal. That's why we believe that even though such attacks will never be widespread, in the next year we expect to see some occurring, especially in retaliation to political decisions.

ADVANCED SUPPLY CHAIN

This is one of the most worrisome vectors of attack, which has been successfully exploited over the last two years, and it has made everyone think about how many providers they have and how secure they are. Well, there is no easy answer to this kind of attack.

Even though this is a fantastic vector for targeting a whole industry (similar to watering hole attacks) or even a whole country (as seen with NotPetya), it's not that good when it comes to more targeted attacks as the risk of detection is higher. We have also seen more indiscriminate attempts like injecting malicious code in public repositories for common libraries. The latter technique might be useful in very carefully timed attacks when these libraries are used in a very particular project, with the subsequent removal of the malicious code from the repository. Now, can this kind of attack be used in a more targeted way? It appears to be difficult in the case of software because it will leave traces everywhere and the malware is likely to be distributed to several customers. It is more realistic in cases when the provider works exclusively for a specific customer.

What about hardware implants? Are they a real possibility? There has been some recent controversy about that. Even though we saw from Snowden's leaks how hardware can be manipulated on its way to the customer, this does not appear to be something that most actors can do other than the very powerful ones. And even they will be limited by several factors.

However, in cases where the buyer of a particular order is known, it might be more feasible for an actor to try and manipulate hardware at its origin rather than on its way to the customer.

It's difficult to imagine how all the technical controls in an industrial assembly line could be circumvented and how such manipulation could be carried out. We don´t want to discard this possibility, but it would probably entail the collaboration of the manufacturer.

All in all, supply chain attacks are an effective infection vector that we will continue to see. In terms of hardware implants we believe it is extremely unlikely to happen and if it does, we will probably never know....

AND MOBILE

This is in every year's predictions. Nothing groundbreaking is expected, but it's always interesting to think about the two speeds for this slow wave of infections. It goes without saying that all actors have mobile components in their campaigns; it makes no sense only going for PCs. The reality is that we can find many examples of artifacts for Android, but also a few improvements in terms of attacking iOS. Even though successful infections for iPhone requires concatenating several 0-days, it's always worth remembering that incredibly well-resourced actors can pay for such technology and use it in critical attacks. Some private companies claim they can access any iPhone that they physically possess. Other less affluent groups can find some creative ways to circumvent security on such devices using, for instance, rogue MDM servers and asking targets through social engineering to use them in their devices, providing the attackers with the ability to install malicious applications.

It will be interesting to see if the boot code for iOS leaked at the beginning of the year will provide any advantage to the attackers, or if they'll find new ways of exploiting it.

In any case, we don´t expect any big outbreak when it comes to mobile targeted malware, but we expect to see continuous activity by advanced attackers aimed at finding ways to access their targets' devices.

THE OTHER THINGS

What might attackers be thinking about in more futuristic terms? One of the ideas, especially in the military field, might be to stop using weak error-prone humans and replacing them with something more mechanical. With that in mind, and also thinking of the alleged GRU agents expelled from the Netherlands last April after trying to hack into the OPCW's Wi-Fi network as an example, what about using drones instead of human agents for short-range hacking?

Or what about backdooring some of the hundreds of cryptocurrency projects for data gathering, or even financial gain?

Use of any digital good for money laundering? What about using in-game purchases and then selling such accounts later in the marketplace?

There are so many possibilities that predictions always fall short of reality. The complexity of the environment cannot be fully understood anymore, raising possibilities for specialist attacks in different areas. How can a stock exchange's internal inter-banking system be abused for fraud? I have no idea, I don´t even know if such a system exists. This is just one example of how open to the imagination the attackers behind these campaigns are.

We are here to try and anticipate, to understand the attacks we don´t, and to prevent them from occurring in the future.