Avast Threat Landscape Report

2019 Predictions

Contents

Introduction A

A Introduction
Threat Landscape 2018

In 2018, we celebrated the thirtieth anniversary of the World Wide Web; it was also Avast's 30th birthday. Back in 1988, one of Avast's founders received a floppy disk containing the infamous Vienna virus and was inspired to study and conquer it. Fast forward thirty years, and we are still driven by the desire to protect people's digital life, a passion that was founded in a deep belief that security and privacy are a fundamental human right.

In 2018, the threat landscape is exponentially more complex and the available attack surface is growing faster than it has at any other point in the history of technology. PC viruses, while still a global threat, have been joined by a multitude of malware categories that deliver more attacks. People are acquiring more and varied types of connected devices so in addition to a laptop and phone, they have a host of smart devices that power everything from their thermostat to their door locks, which in turn increases the attack surface for threats. Looking ahead, these trends point to a magnification of threats through these expanded threat surfaces.

Average monthly attempted attacks on devices protected by Avast

43M

2M

508K

Types of attacks blocked monthly by Avast

1.5B
Attacks on PC

171M
Files blocked

386M
Web attacks blocked

A Introduction

Looking to 2019

A chain is only as strong as its weakest link. This is also true in the world of security. In 2018, we tracked a key growing threat trend - that when just one device in a home or small business (usually the router) is compromised, then the rest of the devices on the network become easy to compromise. With connected devices - known as the Internet of Things - growing faster than any device category in history, it's increasingly difficult to buy appliances and home goods that do not have some connection over to the internet.

From connected lights to coffee makers, and smart speakers to toothbrushes, IoT devices will continue to drive a class of attacks aimed at exploiting their weaknesses in configuration, security flaws, and consumers' low engagement with their security settings. In 2019, we will see more attacks aimed at infiltrating an IoT device as this could easily lead to breaking into the perimeter where IoT devices with compromised modems reside.

Key trends

Sophistication: malware authors will again up the level of sophistication of their wares. We will see multi-purpose malware platforms, with better self-defense techniques, that could potentially do far more damage than Distributed Denial of Service (DDoS) or cryptomining attacks.

Cryptomining: this was the most prominent threat in 2017 thanks to a tremendous activity surge coinciding with the escalation in cryptocurrency value in late 2017 and early 2018. While attack levels have fallen with the decline in coin values, we believe that in the future malicious mining will become a game of scale not tightly tied to the value of the currency.

Trojans: with the decline of ransomware following the neutralization of leaked NSA zero-day exploits, criminals turned to fresh exploits to help them monetize their attacks. Therefore, we are tracking a resurgence in banking trojans targeting PCs and mobile devices.

Mobile: similar to the banking trojans, we also tracked an upsurge of fake apps in 2018. These were created faster than they could be identified and taken down. While we expect to see mobile attacks evolve, the relative ease of IoT attacks may continue to cause some criminals to change tactics.

Supply chain: as connected devices are increasingly built from open source code and inexpensive components, there will continue to be profitable supply chain hacks. The lack of security controls in the supply chain and consumer demand for low cost connected devices will open a Pandora's box of potential for hacking components and core software.

Adversarial AI: the rise of adversarial Artificial Intelligence continues to haunt the corners of the threat landscape. Rather than direct, fast evolving, movie style AI assaults we foresee the emergence of a class of attacks known as 'DeepAttacks', which use AI generated content to subtly evade existing AI security controls.

A Introduction

About Avast Threat Labs

The Avast Threat Labs monitor and protect our users from the latest threats. We see roughly one million new files a day and prevent two billion attacks every month. This scope gives us valuable insights and knowledge of the most prevalent threats, allows us to quickly protect against emerging threats and provides us the ability to map trends that allow us to try to predict future threats as well. Every year we take stock of the year that is ending, and we speculate about what the year to come may bring. In this report, we share our top threat predictions for 2019, including ones from 2018 that will continue to present challenges this year.

Internet of Things B

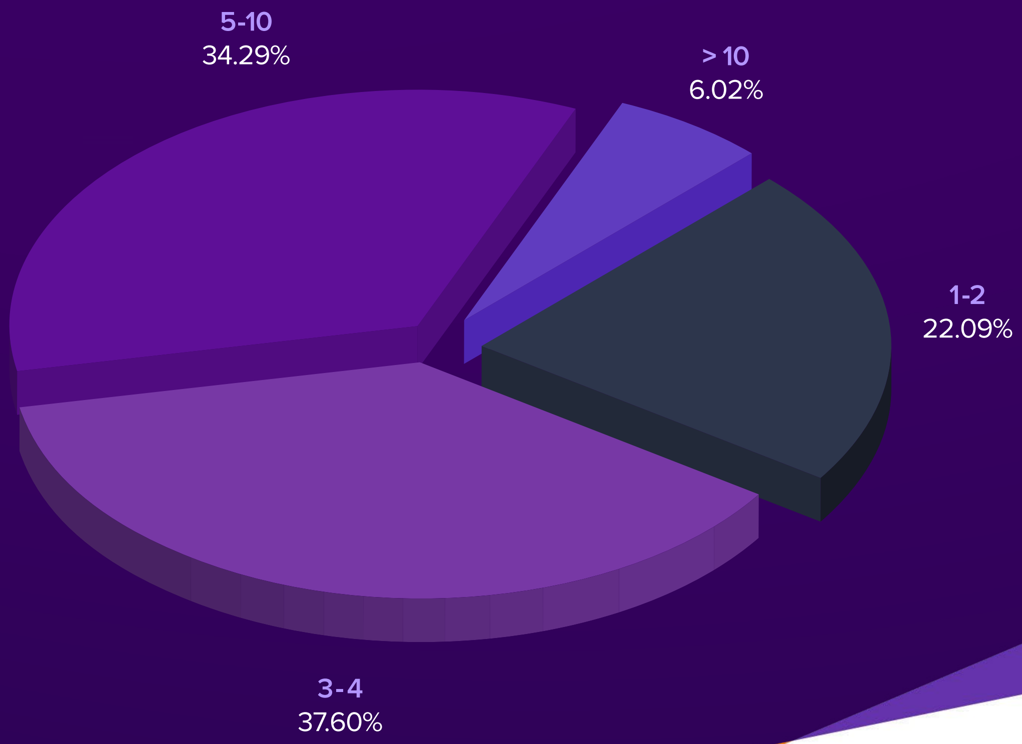
B Internet of Things

The Internet of (Vulnerable) Things

The Internet of Things (IoT) are physical devices, vehicles, home appliances, and other items connected to the internet. According to Juniper Research, the number of connected devices is expected to top 38.5 billion by 2020. The fast growth is because a person may have one laptop and mobile phone, but also a multitude of connected devices in their home from doorbell, to entertainment, to home security system. The trend toward smart devices will be so pronounced in the coming years that it will become difficult to buy appliances or other electronics that are not connected to the internet.

Only two or three years ago, the topic of IoT security was something most people outside of IT security circles had never even heard. The Mirai botnet attack of 2016 changed that, and suddenly people were aware that their devices' processing power could be used for DDoS attacks. In 2018, malicious cryptomining attacks became the attack of choice, but IoT device attacks are still in their infancy.

Number of devices per home network (global):



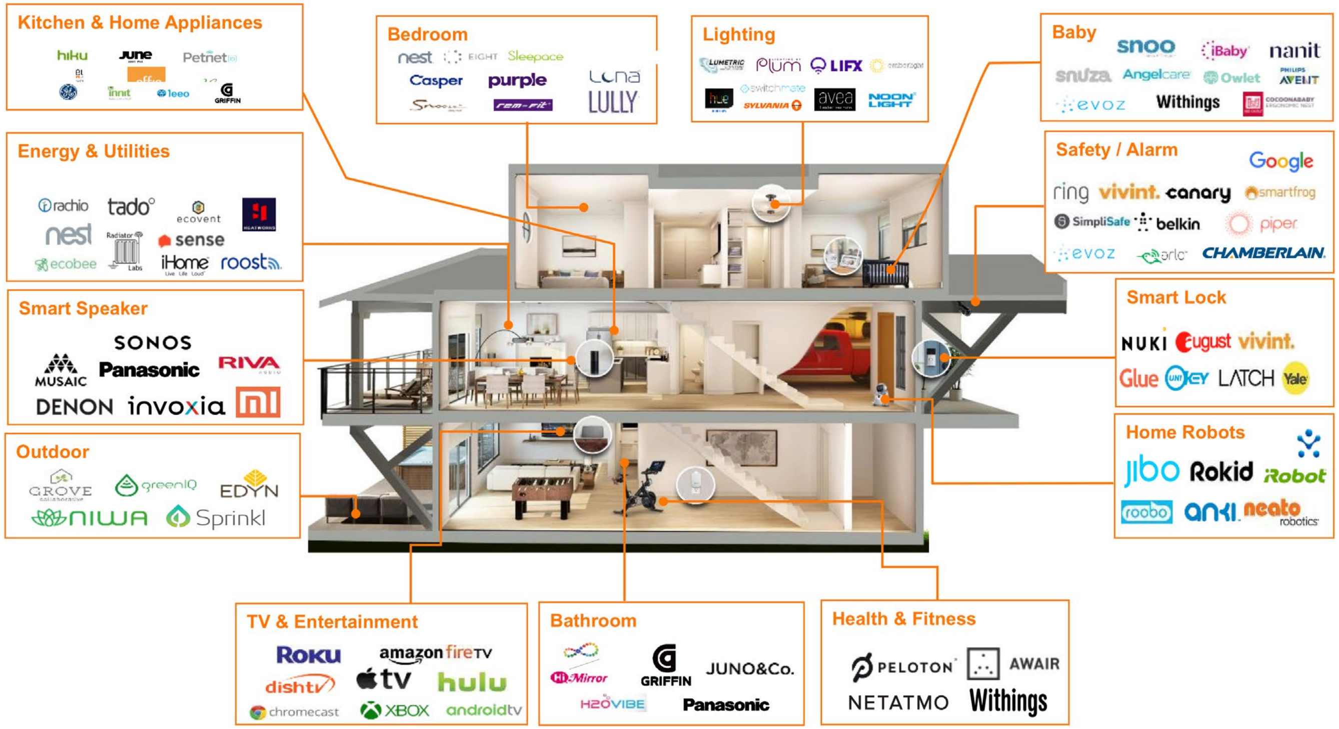
B Internet of Things

The Internet of (Vulnerable) Things

As much of our research has shown, security is often an afterthought in the manufacturing of these devices. While the biggest brand names smart devices often come with embedded security options, some producers skimp on security either to keep costs low for consumers or because they are not experts in security. Considering a smart home is only as safe as its weakest link, this is a mistake.

History tends to repeats itself, and so we can expect to see IoT malware evolve, becoming more sophisticated and dangerous, similar to how PC and mobile malware evolved.

What a house may look like in five years:



B Internet of Things

Router-based Attacks - the worst is yet to come

Anyone whose home is connected to the internet has a router to which they can connect their computers, phones, and IoT devices. Routers are ubiquitous devices - important but rarely maintained to the latest security standards. In fact, once an internet service provider has installed it, most people never give their router a second thought, unless they experience internet disruptions. Avast research shows that 60% of users around the world have never updated their router's firmware, leaving them potentially vulnerable to fairly simple attacks that exploit firmware vulnerabilities.

Infected routers don't necessarily show signs of weakness. When an attacker uses a known vulnerability or weak authentication credentials to access a router, they can gain access not just the router but to all the devices connected to the network. Many users, therefore, may not be aware that their home network has been infiltrated. Routers have proven to be a simple and fertile target for a growing wave of attacks. While many attacks against routers use variants based on the Mirai codebase (which was released by the creator shortly after the successful attacks of September 2016), many are far more complex and point to a murky future for home network security.

Not only have we seen an increase in router-based malware in 2018, but also changes in the characteristics of those attacks. Where router-based malware has traditionally taken over a device for the purposes of carrying out a DDoS attack, such as the Mirai attacks, today's attacks use malware that infects a device and then opens up a line of communication to a command and control server without taking any immediate action.

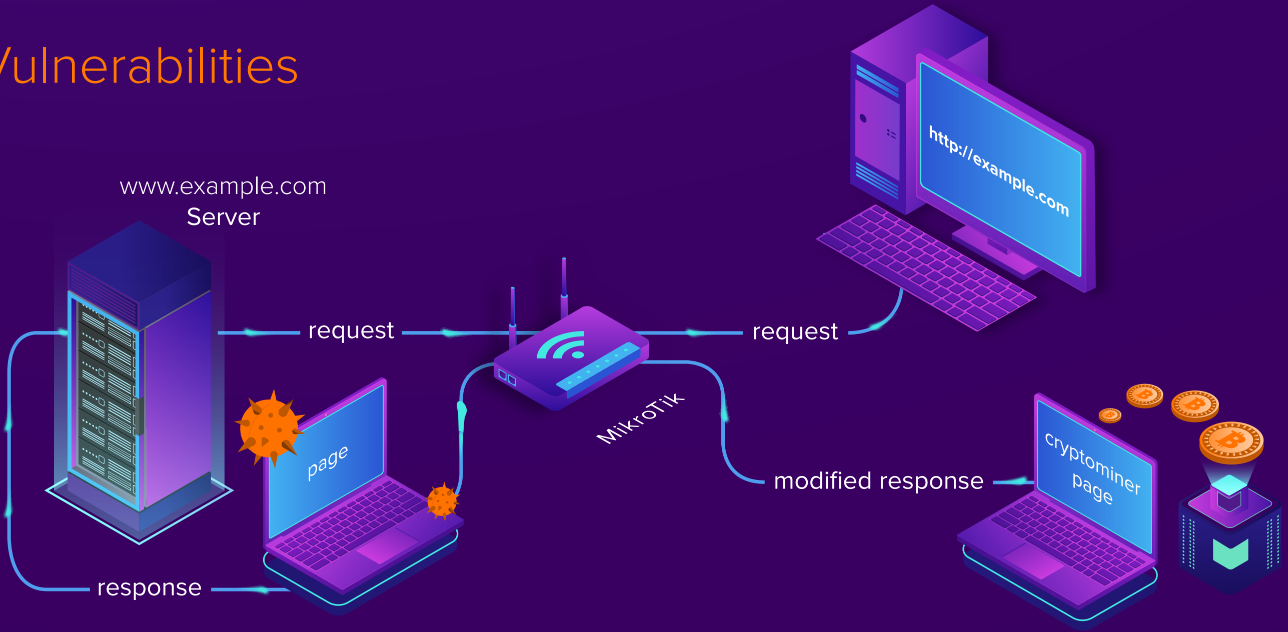
We saw this with VPNFilter and Torii; once the router is infected, these malware strains listen to the network traffic, fingerprint the network and the devices on it, and allow for the command and control server to send new payloads or instructions to the device. In this, the malware acts more like a platform and less like a virus. This 'platform-ification' of IoT malware opens up many possibilities for bad actors who can re-purpose it for a multitude of nefarious activities including pay per install, DDoS for hire, cryptomining, or even good old-fashioned spam. This evolution replicates how PC malware counterparts have evolved and indicates the sophistication of new strains of IoT targeted malware.

In 2019, we expect to see hijacked routers used to steal banking credentials, for example, where an infected router injects a malicious HTML frame to specific web pages when displayed on mobile. This new element could ask mobile users to install a new banking app, for instance, and the malicious app will then capture authentication messages. In 2018, we observed a content injection method with coinmining elements on Mikrotik routers, and in 2019, we expect to see this both escalate in number and to diversify in how content injection capabilities are used.

B Internet of Things

Downstream Effects of Router Vulnerabilities

Routers will continue to be used as targets of an attack, not just to run malicious scripts or spy on users, but also as a intermediate link in chain attacks, as we saw in case of the Mikrotik campaigns where just by re-configuring the router the entire internal network was affected. With Mikrotik, the malware served JavaScript miners to all the browsers behind the router. As these routers are not just in our homes but are also used by many smaller internet service providers, this attack indicated the worrisome potential for an infected router to go on to infect thousands of downstream devices. In such a scenario, it would be very difficult to figure out where the infection is coming from.



Schematic of miner injection into every request made to an HTTP page by any device behind the router

More Modular IoT Malware

Just as PC malware was very simple in its infancy, most IoT malware was originally built for a very narrow purpose such as to gather botnets to launch a DDoS attack. But as with PC malware, IoT malware authors are learning and adjusting their modus operandi from building one trick malware to building multi-purpose malware platforms capable of supporting organized pay per install campaigns, as already mentioned. There are benefits to infecting and then keeping a low profile rather than immediately monetizing the network. After gaining control of a large volume of IoT devices, malware authors can repurpose bots within botnets to do whatever they see fit (or whatever would be most profitable). We have seen this already with malware like Torii and some of the newly researched attacks on Mikrotik routers. Once the device is under the control of the botnet, it can be repurposed to do anything from DDoS to cryptomining or more.

B Internet of Things

More Sophisticated Spreading Techniques

We expect to see more browser-based malware targeting IoT devices. Browser-based attacks on personal computers and mobile phones, called Cross Site Request Forgery, are found in the wild but are not yet very common. In this scenario, a user visits a page with malicious Javascript which will scan the user's local network, find a vulnerable device, and infect it. It could be a valuable way to infect a device that is not visible from the internet, for example, a device behind a NAT (Network Address Translation) where the router translates all the devices in a private network into one public IP address on the internet.

IoT Malware as Proxy

Right now, IoT malware authors typically monetize their deeds through cryptomining or DDoS for hire attacks, but this is not the most profitable approach. We think more IoT malware authors will use their position to spread to the more powerful and interesting devices like mobile phones, tablets and PCs. An example of this would be infecting a router to inject JavaScript or any other malicious payload into the traffic delivered to the user. It could also be used as a proxy to connect and carry out attacks on other internet users or devices; by using a chain of such infected devices that barely have any logging capabilities, attackers could disguise their original location, similar to how anonymization proxies work.

IoT Malware Will Drop Support for x86 Architecture

x86 is one of the most common backwards compatible instruction set architectures and has been in use since Intel introduced it in the late 1970s. However, as more devices operating on alternate architectures become available, we are seeing that most botnets operate on other architecture today and therefore predict malware authors will stop including the x86 step to make reverse engineering harder for security vendors.

However, as most malware analysts and tooling are still focused on the x86 architecture, this has effectively created a technological 'debt' in regards to modem platforms. For example, without such rich tooling for ARM or MIPS versions, malware authors skipping x86 will find it much more difficult to develop compatible malware without the ready knowledge and tooling base. There are many sandboxes for PEs (portable executables) and x86 ELFs, but the majority of them struggle to support other architectures.

Extending the Browser Attack Surface

C

C Extending the Browser Attack Surface

Millions of users were affected by malicious browser extensions in 2018, resulting in stolen credentials, increased click fraud, and the spread of cryptominers. We expect this trend to accelerate meaningfully in 2019 as word spreads that successful attacks can be carried out on the browser and consequently the popularity of the browser as an attack surface grows.

Google's Chrome Web Store in particular has proven itself continually vulnerable to penetration by bad actors, despite efforts by Google to stop their spread. Given the large number of extensions and the fact that they can be updated remotely by developers, this becomes a difficult and ongoing security challenge to solve. Users should exercise caution in downloading extensions only from reputable vendors who they independently trust and verify. As the larger browser market consolidates around the Chromium open source project, we expect independent companies other than Google to develop solutions for this problem.

MOAH (Mother of All Hacks): Supply Chain Attacks

D

D MOAH (Mother of All Hacks): Supply Chain Attacks

In 2018, the trend of supply chain hacks we saw in 2017 seemed to escalate with notable hacks including ones targeting open source repositories and HTTP only download portals. In a cover story bombshell, Bloomberg reported that China placed rice-grain-sized chips on the processors of servers that were installed at companies such as Apple and Amazon. The allegation has still not been formally proven or refuted, but it revived the discussions of how insidious a supply chain hack could be. What puzzles us about this report is that this supply chain hack is far more complex than it needed to be. Many experts have pointed out that if a hacker wanted to infiltrate the infrastructure of these companies and identify the hardware they were using, it could have more easily attacked the known vulnerabilities on that infrastructure, rather than intercept and interfere with the hardware along the way.

The fact is that supply chain hacks are very easy and will still become easier. Commodity chipsets are added into new devices every day, and a simple hack on one of those components can potentially crack hundreds of thousands of devices. As malware morphs off traditional platforms like x86 onto IoT platforms like ARM, we will see such attacks amplified because they involve a component of many popular devices.

We demonstrated how to take over a coffee maker at the IFA Plus Summit in Berlin last year; the point was not so much to show that we can ransom a coffee maker, but to show what attacks on the firmware of certain components could do. It's common for Wi-Fi enabled smart devices to use commodity ready-made Wi-Fi modem modules. These modems usually contain their own firmware and are quite often more powerful than the main CPU of the device. Many IoT device vendors are broadly using them, making them the perfect target for Advanced Persistent Threat (APT) attacks. Imagine someone replacing the firmware in a component that carries out the majority of communication between the device and internet. Infiltrating such a device could easily lead to breaking into the perimeter where IoT devices with compromised modems reside. Most people wouldn't suspect their coffee machine to leak their personal or even worse, company data.

We are used to seeing APT attacks mostly through trojanized software. But the rise of IoT devices and adoption of these not only by consumers, but also by companies, we'll more likely see rise of APT attacks carried out by compromised coffee machines, TVs, fridges, security cameras or even attendance systems.

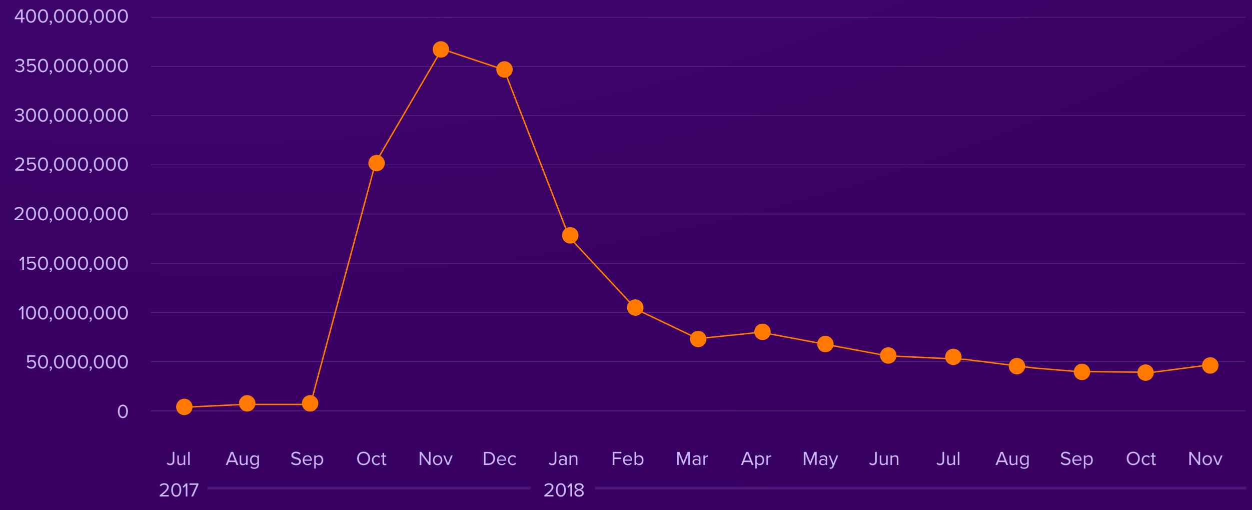
Monetizing Threats

E

E Monetizing Threats

Ransomware dominated 2017, but in 2018, bad actors returned to familiar monetization methods. Without the flashy exploits from Shadow Brokers' NSA zero-day trove, ransomware waned, but it is still a successful form of attack. In 2019, we expect to see old school monetization attacks like those outlined next prevail.

Global Cryptojacking Trend



Cryptojacking Becomes a Game of Scale

Cryptojacking has been one of the most widespread threats in 2018, and we expect cybercriminals to broaden their attacks in this field, particularly as the attack surface increases with every new IoT device that goes online.

One could think that as the most popular cryptocurrency value has dropped dramatically in the last year, that attackers would lose interest in cryptojacking. There does in fact seem to be a correlation between the price of cryptocoin and the level of malicious cryptocurrency mining; however, that doesn't mean that the price of currency will always influence the rise and fall in mining activities. Though there was a spike in malicious mining that coincided with the last major increase in the Bitcoin's price, we believe that the overall size of the IoT attack surface will be the more accurate indicator of mining levels in the future. Cryptomining is the lazy hacker's monetization strategy. An Avast survey showed that 60% of consumers worldwide have never updated their router or reset the router's default password, making brute force attacks very simple. Routers are open to attack and using a victim's computer power is free of cost for the attackers. Unlike most forms of cybercrime, once it is deployed it does not require any extra work, cybercriminals can just sit back and watch their wallet grow. With a readily available piece of code, they can target all kind of devices, from routers to IP cameras, which makes it the greatest attack surface of which they could dream. Furthermore, embedded smart devices typically have much less computing power than PCs, so their biggest advantage is the time dimension. Infecting a PC with a cryptominer means the infection typically doesn't last very long because the user will notice something is wrong and many security solutions detect PC cryptojacking. In case of smart devices, however, the malware can sit on the device for many months or even years, undetected and mining round the clock.

Cryptomining levels in the future will be driven more by the availability of devices recruited, and less by the price of the currency. Recent price drops have shown that cryptomining may not be profitable enough to support a cybercriminal, but if one controls enough devices, the results could be an attractive passive income stream.

E Monetizing Threats

Attacks on Cryptocurrencies, Not Just Exchanges

More heists and attacks will be carried out directly on exchanges, but it is also possible that we will witness even more serious attacks, such as a 51% attack, on some of the cryptocurrencies like the one recently live streamed by a cryptocurrency researcher.

Renaissance of Banking Trojans

Banking trojans, also known as bankers, are nothing new. They are malicious programs that try to gain access to personal and confidential information through online banking and payment systems. They have been with us for more than a decade, stealing credentials and siphoning funds from consumer and business bank accounts. However, they were unjustly overlooked during the last three to four years, as ransomware and malicious cryptominers became popular.

Despite banking trojan activity being lower than usual in the past few years, they are returning at full strength, with strains like as Emotet or Trickbot. We expect 2019 to be the renaissance of banking trojans and not just on personal computers and mobile devices, but also on IoT devices. We particularly expect banking trojans to target mobile devices, as SMS interception allows cybercriminals to more easily bypass two factor authentication methods. Since most banking authentication codes are sent to mobile devices, these become the main targets for bad actors to collect them. With the decline of profits from cryptominers and ransomware, we can expect to see banking become a more popular target for cybercriminals.

What About Ransomware

While ransomware attacks have declined overall after 2017s headline grabbing attacks, that doesn't mean ransomware is no longer a problem. Attacks on consumers have decreased, but attacks against businesses are becoming more popular, as attackers are focusing on victims that can improve their return of investment. Once they compromise an endpoint in a targeted company's environment, that attacker can identify all the computers on the network to launch a full-scale attack. While the chance that a business will pay ransom for a single computer is rather low, if the attack compromises multiple computers on a network then the likelihood of the ransom being paid increases - additionally, the ransom amount cybercriminals demand will also grow exponentially.

A ransomware attack of this kind requires a very broad skillset to execute, as it usually calls for knowledge of many different areas of security. Planning an attack like this takes time, but can be very profitable. In 2018, we saw an attack called SamSam successfully target the healthcare sector. Traditionally, the healthcare sector is poorly secured, running outdated hardware and operating systems, and lacking sufficient IT resources to address potential issues, making it easy target. We predict more well-targeted attacks carried out against vulnerable sectors which will need to invest in extra precautions to protect their environment.

Mobile F

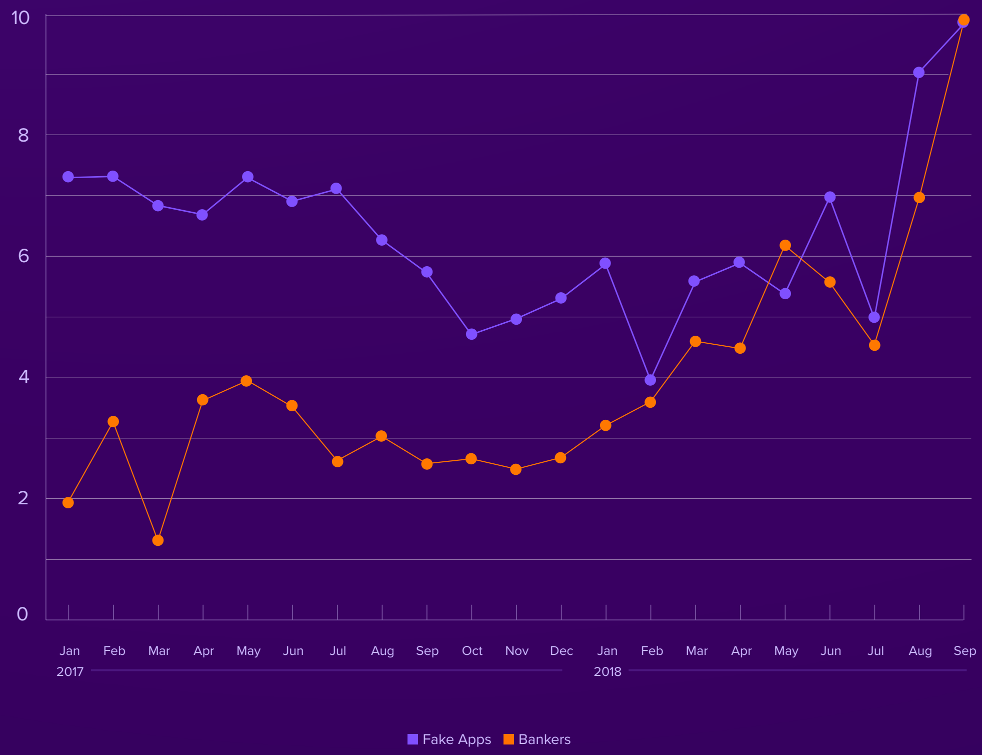
F Mobile

Mobile threats are on the decline overall thanks to better native Android security protections. Comparing 2018 to 2017, there were 60 percent fewer attacks, owing largely to significant drops in attacks that attempted to gain root access to a device, known as 'Rooters', which fell 77 percent. 'Clickers' declined by 57 percent and 'downloaders' fell by 10 percent. Most other categories had slight to moderate inclines, with aggressive ad-based malware increasing 49 percent and fake apps increasing 24 percent.

In 2018, the return of banking trojans was particularly pronounced on the mobile side, growing 150 percent YoY, from 3 percent to over 7 percent of all detections we see worldwide. While perhaps not a big shift in terms of the overall volume, we believe that cybercriminals are finding bankers to be a more reliable way to make money than cryptomining.

In 2019, we expect to see well-known tactics such as advertising, phishing, and fake apps continue to dominate the mobile threat landscape.

Percentage of fake apps and bankers Avast detected



Fake Apps

In 2018, we tracked and flagged countless fake apps using our apklab.io platform, some were even found on Google's Play Store. Fake apps are like the zombies in mobile security, becoming so ubiquitous, they barely even make the news as new fake apps pop-up to take the place of ones already flagged for removal. They will continue to persist as a trend, exacerbated by fake versions of popular app brands making their rounds on the Google Play Store.

F Mobile

Play Store Defections Create Security Gaps

One of the most controversial things to happen in terms of Android security in 2018 was game maker Epic offering their popular game, Fortnite, for download outside the Google Play Store; a move it is thought was made because of the cut Google takes from app developers for distributing apps on the Play Store.

We will likely see more game studios follow Epic’s lead, despite the negative feedback the security industry gave on how safe this is for users. There is nothing to stop cybercriminals from uploading malware-laden versions of the app to third party Stores that don’t have the verification resources Google does to ensure an app is safe and genuine. That being said, even in the well-policed Google Play store, we still found a lot of malware in available apps in 2018.

Router infection via Android Devices

While we have seen some sophisticated malware hiding and operating stealthily in the background, the apps that seem to gain the most traction these days are apps whose main purpose is to monetize by overloading users with ads and the distributing suspicious payloads, like a banking trojans and SMS stealers. We touched on the router based attacks of 2018 and how we believe they will evolve into sophisticated malware platforms. We can expect the infection vector to evolve - via Android devices. We believe that we will see purpose built malware targeting routers via mobile devices in 2019.

Smishing for Gold

Smishing is another area that has recently generated intense interest, partly because it is allegedly carried out by privately created and contracted state sponsored malware. The latest example, which is very high profile, is an exploit of the Pegasus software from thte NSO group Pegasus was used to target specific Saudi citizens, and at the time this piece was written, the malware’s role in the murder of journalist Jamal Kashoggi is being investigated.

Smishing is phishing via SMS with the goal of encouraging victims either into giving up personal information or install spyware. In the past, smishing was used to spread phishing scam links to obtain sensitive information from people, but we now expect smishing to become a major attack vector when it comes to delivering mobile malware, on both the iOS and Android operating system.

<< Contents

Artificial Intelligence & Adversarial AI

G

G Artificial Intelligence & Adversarial AI

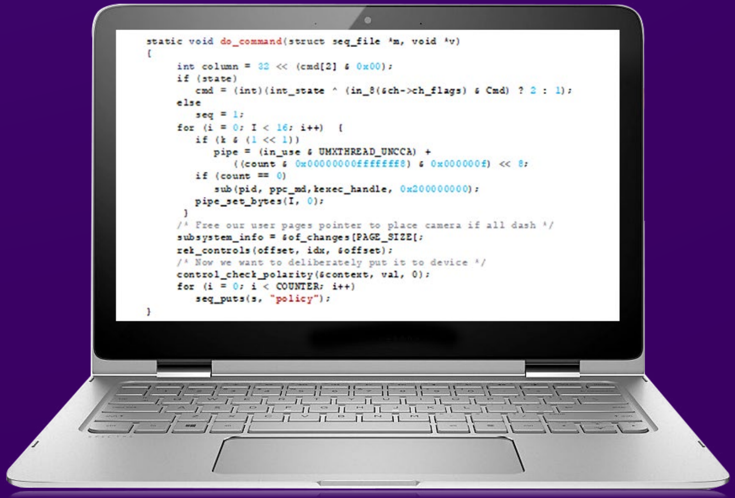
Certainly no area of security carries more mystery than that of Artificial Intelligence. Not only is security the only field in which adversarial AI algorithms are likely to battle AI algorithms, but it is also the area where security stands the most chance for large gain. Avast has invested heavily in developing AI algorithms to combat the forces of adversarial AI, and our learning in this space has led us to research things we know exist, but are not yet fully known or understood. This will help us build AI muscle to defend better against a variety of attacks. One of those areas of early exploration we are calling 'DeepAttacks'.

The Age of DeepAttacks is coming

We define DeepAttacks as 'malicious content automatically generated by AI algorithms'. In 2018, we observed many examples where researchers used adversarial AI algorithms to fool humans. Examples include the fake Obama video created by Buzzfeed where President Obama is seen delivering fake sentences, in a convincing fashion. This is commonly called a 'deepfake' and illustrates the use of AI to trick people. We have also seen examples of adversarial AI deliberately confounding the smartest object detection algorithms, such as fooling an algorithm into thinking that a stop sign was a 45 mph sign. Another AI-generated attack example, called 'fakenews' has rarely been seen in real-life. At the same time, DeepAttacks can manifest themselves, at scale, in the form of fake URLs or HTML webpages. For instance, DeepAttacks can be used to automatically adapt a generic phishing site to a target brand based on learning its visual style from the legitimate homepage. More commonly, malicious domain names are typically generated by DGAs (Domain Generation Algorithms), e.g. by stitching together English words, like bluefieldcows.com. Security teams have been including DGA-detection algorithms in their smart defenses (e.g. Akamai and Aella) for some years but this is an area where DeepAttacks can be used to generate smart and adaptable domain names which avoid the DGA detectors.

DeepAttacks can also be used to generate fake network traffic in botnets, using AI that is trained to avoid detection by known firewalls/IDS. And such Adversarial AI algorithms can be trained to inject superfluous code into a malware sample, until the sample is no longer detected by the target AV engine. Thus, the DeepAttack methodology allows a bad actor to mount an attack using this now undetectable malware, in order to have a much more significant impact. In 2019, we expect to see DeepAttacks deployed more commonly in an attempt to evade both human detections and smart defenses. We are working hard to hone special detections for DeepAttacks, in order to identify and block these before they reach magnified proportions.

Example of AI generated code piece.



```
static void do_command(struct seq_file *m, void *v)
{
     int column = 32 << (cmd[2] & 0x00);
     if (state)
        cmd = (int)(int_state ^ (in_8(&ch->ch_flags) & Cmd) ? 2 : 1);
     else
        seq = 1;
     for (i = 0; I < 16; i++)  {
        if (k & (1 << 1))
           pipe = (in_use & UMXTHREAD_UNCCA) +
              ((count & 0x00000000fffffff8) & 0x000000f) << 8;
        if (count == 0)
           sub(pid, ppc_md,kexec_handle, 0x20000000);
        pipe_set_bytes(I, 0);
      }
     /* Free our user pages pointer to place camera if all dash */
     subsystem_info = &of_changes[PAGE_SIZE[;
     rek_controls(offset, idx, &offset);
     /* Now we want to deliberately put it to device */
     control_check_polarity(&context, val, 0);
     for (i = 0; i < COUNTER; i++)
        seq_puts(s, "policy");
}
```

G Artificial Intelligence & Adversarial AI

Smart Attacks on Home Networks

We've seen how easy it is for a human hacker to exploit machines in the local network when control is taken of a home router or connected device. However, that attack does not scale, as the attacker needs to infiltrate many homes before finding a suitable victim. This is where smart algorithms come in. An attacker can run sophisticated AI algorithms to target scans and identify homeowners with a specific profile (e.g. lots of Apple devices, or with at least 10 vulnerable devices). Then they can automate the next stage of the targeted attack by attacking a desired device, one that, for example, is suitable for cryptomining, using password crackers that adapt to the specific device types.

AI Against Clone Phishing

We predict that AI will play a large role in ending the practice known as clone phishing, where an attacker creates a nearly identical replica of a legitimate message to trick people into thinking it is real. The email is sent from an address resembling the legitimate sender, and the body of the message looks the same as a previous message. The only difference is that the attachment or the link in the message has been swapped out with a malicious one. We predict AI will become effective in dealing with clone phishing attacks to detect short-lived phishing websites. AI can move faster than traditional algorithms in two ways. First, by accurately identifying domains that are new and suspicious. Second, by utilizing fast algorithms from the visual detection domains to match the layout of phishing pages to popular sites, and identify fake ones. And finally, because it can learn over time and follow the trends and improvements attackers make.

Sadly, targeted spearphishing techniques will continue to be successful as attackers spend time and money to gather target-specific information to create an email purporting to be coming from a familiar and trusted person. In these instances, as in many others, a highly motivated attacker will often find a way in and it's up to other detection technologies, like behavioral engines, to stop the threat.

End of Text Captchas

For over a decade, humans proved they aren't robots by reading text letters and transcribing them correctly. This was the most effective tool to ensure that a bot wasn't active, but now text captchas are no longer as effective as they once were. Late 2017, Vicarious, a company developing AI software, showed that even complex captchas can be broken by algorithms. This has led to the introduction of behavioral analysis to identify bot activity on websites by generating a risk score on how suspicious an interaction is and ending the need to challenge users to enter distorted text in a box to prove they are a person. Even Google's Recaptcha, which is the biggest provider of captchas is moving away from text-based captchas. Recaptcha's technology has been adopted quickly, and with it's proliferation, the end of text captchas will come in 2019.

Contact Information

pr@avast.com