2020 Threat Landscape Report

Introduction

The Avast Threat Labs monitors and protects our more than 400 million users worldwide from the latest threats. Avast detects threats in near real time and blocks about 1.5 billion attacks a month. This scope gives us valuable insights into, and knowledge of, the most prevalent threats which allows us to quickly protect against emerging threats, and provides us with the ability to map trends that allow Avast experts from various fields to try and predict future threats as well.

For 2020, we predict advancements to be made in terms of how malware is delivered to PCs, including: more sophisticated methods of spreading threats via malicious emails; through a resurgence of exploit kits; via supply chain attacks; and by abusing the Remote Desktop Protocol (RDP).

On the mobile side, we predict that more subscription scams and fake apps will make their way onto official app stores, and that more iOS vulnerabilities will be exposed by researchers and bad actors alike.

In terms of Internet of Things devices, we predict devices and even physical locations will become smart or even smarter than they already are. We have already started to see cybercriminals taking steps to further develop IoT malware, including adding obfuscation to make it more difficult for analysts to analyze, and building upon exploit kits for smart devices.

Finally, we expect privacy will become the new frontier for security, especially when it comes to big data collected for AI algorithms.

Table of contents

PC

More sophisticated spreading of malware by emails

For more than a decade, malicious email spam, also known as malspam, was one of the primary ways cybercriminals spread malware. At the same time, antivirus companies, and email providers alike have heavily invested in spam filtering, greatly improving the detection of malicious attachments, and more. This in turn has caused adversaries to continuously innovate to better their chances of reaching potential victims.

Earlier this year, the banking trojan Emotet, which has been around since 2014, began spreading using a new technique. In addition to spreading via malspam, Emotet began scanning victims' email inboxes and replying to emails, including malicious attachments, and thus infecting further users.

Similarly, there have been cases of malware creating stealthy filters on email servers to steal new incoming messages, to either spy on victims, or to add a malicious payload to the email to then send back into the conversation.

Furthermore, there is an entire cybercrime business focused on stealing and reselling SMTP (Simple Mail Transfer Protocol) credentials, which are the same credentials used to log into an email account. SMTP is used by email clients to send emails, and using stolen SMTP credentials, cybercriminals can send malicious emails appearing to be from specific people.

We predict emails will continue to be the number one mechanism to spread malware, but we expect the methods used to send them will become more sophisticated, and that cybercriminals will begin using adversarial AI to prepare and send emails with malicious or phishing content or attachments.

PC Predictions

Resurgence of exploit kits

While email is and will most likely remain the primary method to spread malware, there are other more sophisticated methods we predict will be taken advantage of within the next year. One of them is exploit kits.

Exploits are code that take advantage of vulnerabilities, and exploit kits are programs that exploit multiple vulnerabilities. Exploit kits are used by cybercriminals to gain access to devices, mainly via malvertising.

When someone visits a site with malvertising running an exploit kit, the kit searches for vulnerabilities in the software the visitor uses to deliver and execute malware, such as trojans, or ransomware. Many cybercriminals rent out exploit kits on the darknet for further cybercriminals to abuse. Some of the most active exploit kits we have seen during 2019 were RIG and Fallout, which are offered as a service from anywhere between $700 USD to $2,000 USD a month.

In the past, exploit kits used to be one of the main methods of spreading malware, however, from 2016 - 2017, the exploit business appeared to be on a decline. However, in the past two to three years, exploit kits have undergone heavy development, and cybercriminals are now adding new exploits and techniques to evade antivirus detections, including detecting virtual machines and malware analysis tools.

In 2019, we also saw an increase in router exploit kits, mainly targeting Brazilians, but also local U.S. and Canadian Internet Service Providers. We expect to see an increase in the amount and sophistication of exploit kits, targeting PCs and routers in 2020.

PC Predictions

Supply chain attacks will continue to make headlines

We’ve been predicting an increase in supply chain attacks for a few years now and have observed their rise over the past two years. We don’t expect this trend to stop.

APT (Advanced Persistent Threat) groups are attempting to infiltrate software companies with massive user bases to inject malicious code into genuine products. The motivation behind supply chain attacks often differs. We have observed cases where just a fraction of the affected user base is the actual target of a supply chain attack. This was the case in the CCleaner attack in 2017, and in the ASUS supply chain attack in 2018.

On the other hand, there are cases where the motivation behind supply chain attacks is mass destruction, like with the NotPetya attack. Cybercriminals spread the NotPetya ransomware, more precisely wiper, by compromising Ukrainian account software, M.E.Doc.

PC Predictions

RDP: Innocent until used for evil

The Remote Desktop Protocol (RDP), a feature included in every Windows version since XP, is used to allow remote access from one machine to another, e.g. an employee working remotely can access a workstation or server located in their company. It could be as simple as running RDP client software on a laptop and connecting to a machine with the RDP server counterpart. RDP then provides an encrypted connection between both endpoints. The usefulness of connecting remotely to a desktop using RDP has changed the way much of the world conducts business. It is, unfortunately, also one of the most attractive methods for cybercriminals to infiltrate a victim's network and deliver the malicious payload.

In the past, cybercriminals have either brute-forced, or guessed, weak credentials to gain access. With newly discovered RDP vulnerabilities, such as BlueKeep, there are even more opportunities for cybercriminals.

In the past few years, cybercriminals have abused the feature to distribute ransomware to small and medium businesses.

In 2020, we expect to see a significant increase in all types of attacks on RDP.

We are likely to see cybercriminals abusing weakly configured servers with RDP as well as exploiting RDP vulnerabilities - whatever will be more profitable for them at a time. The majority of delivered malicious payloads will probably still be ransomware, but we expect a rise in distribution of coin-miners and password stealers. We also expect to see the spread of worm-like strains similar to WannaCry.

PC Predictions

About Jakub Kroustek

Jakub is Head of the Threat Intelligence Systems at Avast. Jakub is a passionate malware hunter and researcher with a love of reverse engineering. His expertise lies in ransomware, botnets, and automating all the boring stuff.

Jakub hates malware, but enjoys analyzing it and spreading the word about his findings including presentations on conferences such as Virus Bulletin, CARO, or Botconf.

Jakub holds a Ph.D. degree in Computer Science and Engineering from the Brno University of Technology.

Mobile

Subscription scams and fake apps

On the mobile side, we predict that more subscription scams and fake apps will make their way onto official app stores.

Subscription scams allow people to use an app for free for a limited period of time, and if the subscription is not canceled, the app charges customers higher than usual fees — often on a weekly or monthly basis. We expect we will see subscription scam apps rise on both the Google Play Store and the Apple App Store.

Fake apps, on the other hand, are illegitimate apps posing as benign ones in order to drive downloads, to collect personal data, and expose people to advertisements or malware.

Cybercriminals are resorting to subscription scams and fake apps, as it is difficult to surpass official app store security checks.

iOS jailbreaks opening the door

On the iOS side, based on the latest findings from the iOS jailbreak community, we expect more vulnerabilities will be exposed by researchers and bad actors alike. The checkm8 jailbreak exploit, discovered this year, is a very serious vulnerability as it exploits the first thing that runs on iOS devices when they are turned on, thus allowing access to anything that comes after. Additionally, it can't ever be updated or fixed on the existing devices, as the exploited code is in a read-only memory. The only "fix" is to buy a new device, like the iPhone XS / XR or newer.

While the exploit requires physical access to the targeted device, criminals and even government agencies have gained a new tool for their arsenal.

We are already seeing community projects, like checkra1n, providing high-quality semi-tethered jailbreaks based on the checkm8 bootrom exploit. This could enable researchers to discover more vulnerabilities which, we hope, will be reported to Apple and not used for evil.

Mobile

About Nikolaos Chrysaidos

Nikolaos Chrysaidos is Head of Mobile Threat Intelligence and Security at Avast, leading mobile security projects, mobile threat intelligence, and threat prevention. In his day-to-day work, he drives mobile forensics, malware analysis, reverse engineering, and application penetration testing to stay ahead of current mobile threats and security issues.

Additionally, Nikolaos and his team work on apklab.io, a mobile threat intelligence platform designed to make it easier for security researchers to hunt and analyze mobile malware.

Nikolaos holds a Bachelor of Science in Computing from the University of Wales, and a Master of Science in CyberSecurity from the University of York, and has successfully presented at various conferences such as AVAR, CARO, RSA, BSides, and MWC 360.

Internet of Things (IoT)

Smarter smart devices and places

In terms of the IoT, we predict smart devices will become even smarter, collecting more data about users, to learn and predict user behavior. This will be done to target users with advertisements, similar to how websites collect user data to better target users with ads based on their preferences. We also predict a rise in the number of 'smart supermarkets' like Amazon Go, which track customers, the items they select, and allow customers to walk out of the store without cashing out at a register.

Smart devices and locations that collect data offer convenience but they limit people's control over their privacy. Additionally, companies collecting and storing a plethora of customer data make attractive targets for data hungry cybercriminals looking to sell data for financial gain on underground markets.

More sophisticated IoT malware

We have already noticed cybercriminals adding sophisticated defences to IoT malware, adding obfuscation to their code, similar to how cybercriminals attempt to protect their Windows malware code from being analyzed by researchers, and we expect this to continue as more people adopt smart devices, widening the IoT attack surface.

Internet of Things (IoT)

About Anna Shirokova

Anna Shirokova is a security researcher at Avast, focusing on the IoT threat landscape. Anna has presented at leading industry events including Botconf, Troopers, BruCon, Wacco Workshop, Virus Bulletin, and Black Hat Europe.

Anna also works on the Stratosphere IPS project where she analyzes attacks carried out on IoT devices, and publishes her findings along with other project team members.

Internet of Things (IoT)

RCE exploits

Remote code execution vulnerabilities allow cybercriminals to exploit devices, execute commands, download malware, and gain control of vulnerable devices. Successful botnets have taken advantage of zero-day RCE exploits for particular devices. Nevertheless, n-day exploits, or known exploits, are also effective and used daily, as not every IoT vulnerability is patched and updated fast enough.

As new smart devices are introduced to the market, new exploits are developed and released and malware authors can build upon older, already established malware families, expanding them with newly released exploits to widen their IoT attack surface. We expect this trend to continue and predict that large botnets will be even easier to build in the future.

Botnet infrastructure

Malware authors have been making progress in preparing their attack infrastructure. The 'state of the art' botnets have progressed from the early-days of IoT malware with hard-coded C&C servers to become well-designed fully-fledged networks using a variety of techniques, both client-server and peer-to-peer based. We have seen IoT malware adopting DNS-over-HTTPS, Tor communication, proxies, and different encryption methods, and we expect malware authors will adopt other security practices to make their networks more robust.

We also expect to see progress when it comes to botnet monetization. Although DDoS attacks and cryptocurrency mining are still the most popular uses of botnets, we foresee more specialized botnets for proxying, information gathering, or eavesdropping will appear in 2020.

Internet of Things (IoT)

About Daniel Uhricek

Daniel Uhricek is a security researcher at Avast. Daniel works on multiple areas within IoT threat research. His expertise comes from tracking IoT malware on a daily basis and developing tools to hunt and analyze malware. His interests include Linux, networking, and data analysis.

Daniel is currently a Master's student of Computer Security at the CTU in Prague, Czech Republic.

Artificial Intelligence (AI)

Privacy will become the new frontier for security

The general public and legislature are becoming aware of the dangers of a society with little privacy, and we are seeing a number of regulation attempts around the world, e.g. in Europe (GDPR), and California, U.S. (CCPA), to provide protection and control over personal privacy. AI has, unfortunately, been a major driver for the harnessing of private data and the resultant lack of privacy.

In the coming year, we will see practical applications of AI algorithms, including differential privacy, a system in which a description of patterns in a dataset is shared while withholding information about individuals, to profit from big data insights as we do today, but without exposing all the private details.

Data ownership

There is recent work, for example, Data Shapley, to attribute value to individual pieces of data provided by users. While we do not foresee a monetization of personal data in 2020 yet, we hope to start seeing initial products that at least allow individuals to control their own data, e.g. to decide whether and which companies can harness data, and what data they can use.

Artificial Intelligence (AI)

About Rajarshi Gupta

Rajarshi Gupta is the Head of Artificial Intelligence at Avast, responsible for Avast's AI products and research.

Dr. Gupta manages data science teams in Silicon Valley and Europe, leading AI-driven malware detection and mobile protection, together with network security for Smart Home, Avast's next-generation IoT security platform.

Prior to joining Avast, Dr. Gupta worked at Qualcomm Research for many years, where he created 'Snapdragon Smart Protect', the first ever product to achieve On-Device Machine Learning for Security. Dr. Gupta has authored over 200 issued U.S. Patents.

Dr. Gupta holds a PhD in Electrical Engineering and Computer Science from UC Berkeley.

Contact:

PR@avast.com