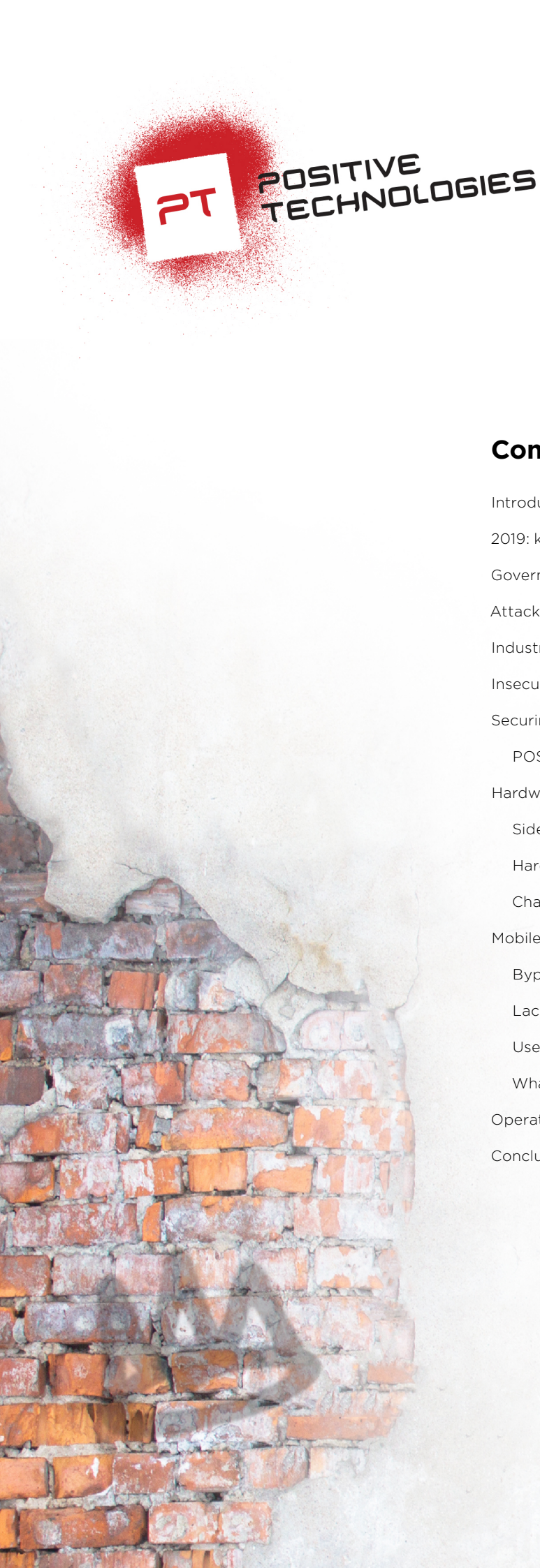
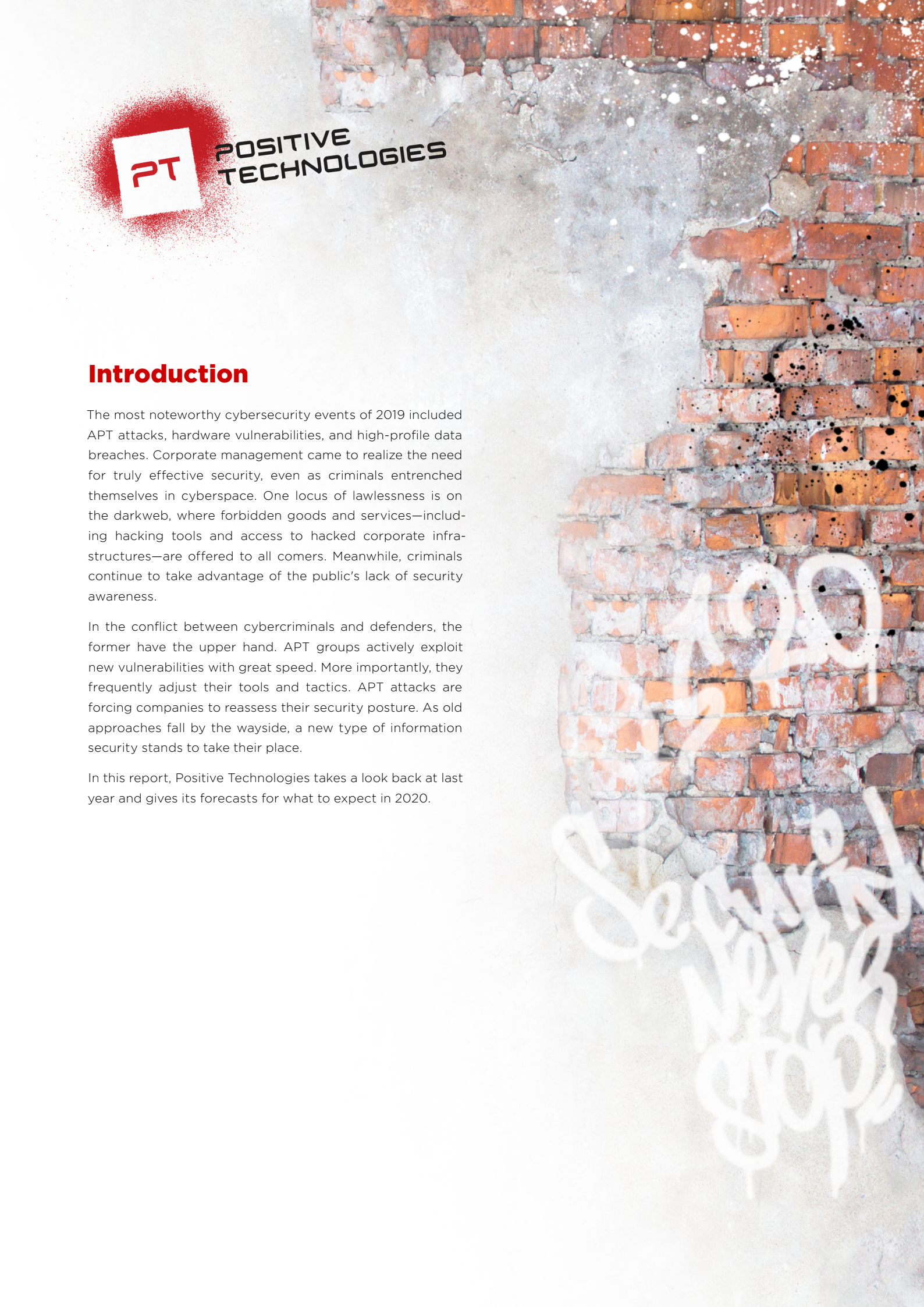
POSITIVE TECHNOLOGIES

Cybersecurity Trends and Forecasts for 2019-2020



Contents



POSITIVE TECHNOLOGIES

Introduction

The most noteworthy cybersecurity events of 2019 included APT attacks, hardware vulnerabilities, and high-profile data breaches. Corporate management came to realize the need for truly effective security, even as criminals entrenched themselves in cyberspace. One locus of lawlessness is on the darkweb, where forbidden goods and services—including hacking tools and access to hacked corporate infrastructures—are offered to all comers. Meanwhile, criminals continue to take advantage of the public's lack of security awareness.

In the conflict between cybercriminals and defenders, the former have the upper hand. APT groups actively exploit new vulnerabilities with great speed. More importantly, they frequently adjust their tools and tactics. APT attacks are forcing companies to reassess their security posture. As old approaches fall by the wayside, a new type of information security stands to take their place.

In this report, Positive Technologies takes a look back at last year and gives its forecasts for what to expect in 2020.

Alexey Novikov
Director of the
Expert Security Center

2019: key security trends

Reports of successful attacks by APT groups frequently appear in the news. All companies, whether or not they make the headlines, are at risk. Nor can they forget about mass attacks, in which large companies are extorted for ransom in return for decryption keys.

In our retrospective analysis and incident investigation work, many companies detect traces of compromises that are months or even years old (last year we detected the TaskMasters group, which had persisted on the infrastructure of one victim for at least eight years). Criminals are in the catbird seat at companies. Victims, overly confident, remain oblivious. We also find in many cases that corporate infrastructure has been "populated" by not just one, but multiple groups.

Thanks to persistent efforts, companies have begun to truly care about information security, detect cyberincidents, analyze hacks, and ask whether their infrastructure is resilient enough. This is certainly a good trend.

But criminals are not standing still. The world of IT is no longer just "virtual." Technology is now part and parcel of the real world. Darkweb markets offer illicit merchandise and services, including hacking utilities. Government efforts to promote user awareness of cybersecurity are haphazard at best. Criminals are easily able to dupe unsuspecting citizens, whether by stealing money or data or by offering too-good-to-be-true earning opportunities.

The barrier to entry for cybercrime is extremely low. Materials for learning how to hack or commit fraud are available on innumerable websites, channels, and messaging platforms.

Cybercriminals take advantage of cryptocurrency. They even create their own dark exchanges to convert money between bank cards and bitcoins. This makes it easy for criminal groups to receive money and anonymize their payments.

In our research on APT groups, we saw growth in the number of APT attacks on various sectors. In 2018, a total of 12 APT groups caught our attention; this number jumped to 27 in 2019. This trend is consistent with our data on constant quarter-over-quarter growth in the number of unique cyberincidents, with 6 percent more unique cyberincidents in Q3 2019 than in Q2. Targeted attacks were significantly more common than mass ones: they picked up as the year went by, growing from 47 percent in the first quarter to 59 percent in the second quarter, and then to 65 percent in the third quarter. This trend is quite likely to continue.

Criminals are making active use of brand-new vulnerabilities (in 2019, APT groups used four zero-day vulnerabilities in their attacks). They act very quickly and, crucially, adapt their tools and tactics. For instance, the RTM group used three different ways to obtain command and control (C2) information: Namecoin, Tor, and Bitcoin. In 2019 we also saw three different versions of the dropper (which installs the main malware module), one version of the loader, and three Trojan versions.

Cobalt is another group targeting the financial sector. Since fall 2019, malware on each infected machine has downloaded an encoded CobInt from the C2 server with unique hash sum for each download: this enables the attackers to avoid hash-based detection of the final malicious file.

One group active in data theft in 2019 used seven different malware versions and four different tactics for persistence and stealth on target infrastructure.

Based on analysis by the Positive Technologies Expert Security Center (PT ESC), groups in 2019 used an average of four malware strains and five tactics for obtaining persistence. Information about APT actions became known as late as 144 months after the fact, with an average of 17 months passing between an attack and public coverage of it.

Thus the key criteria for evaluating the balance of power today between criminals and defenders are:

1. **State-of-the-art attack techniques vs. state-of-the-art defenses: attackers can have an edge of up to three years.**
2. **Use of new vulnerabilities vs. average time-to-patch: attackers nearly always have the advantage, thanks to marshaling exploits in as little as a day.**
3. **Cost of attack vs. cost of defense. Our estimates of the funds needed to acquire software for stealing money from a bank start at $55,000. Cyber-espionage campaigns cost significantly more, with a bare-bones price of $500,000. It is harder to calculate the full cost of protection—equipment, workflows, salaries—due to the wide range of company sizes and maturity levels.**

As ever, APT groups target companies that possess important data and money. These are not necessarily big businesses, but small and mid-sized ones as well, which are used primarily as a stepping-stone to attack larger businesses and disguise attackers' actions.

Telecom companies, vendors, and service providers are increasingly bearing the brunt of attacks. Sometimes companies do not even suspect that a threat could come from that direction. One example we encountered in the field: a supplier of vending machines asked for remote access to perform management via the Internet. The vending machine was connected to the corporate network, which provided Internet access and the ability to synchronize with the supplier's servers. Unfortunately, the client company's internal resources were attacked via this very same channel.

Forecasts

Small to mid-sized businesses—often reluctant to sufficiently invest in cybersecurity—will remain fodder for both mass campaigns and targeted hacks. As large companies strengthen their stance, hackers will have to look beyond advanced phishing and malware techniques, moving to weakly protected partners in order to reach their ultimate targets, perhaps with the help of such partners' special access.

The for-hire criminal market will continue to expand, develop, and evolve. One potentially popular scheme could involve a group hacking corporate infrastructure and breaching the internal network, but not taking advantage of this access for themselves. Instead, they could sell or rent it out to other nefarious players ("Access as a Service"). Operators of malware, such as ransomware, will not have to worry about how to infect corporate systems. They will simply pay a fee for access to already hacked systems. The REvil group (also known as Sodinokibi) already uses this scheme for spreading malware. Pricing for such access may vary based on level. Access to hundreds of network hosts might cost between $3,000 and $5,000, for example, with full control of corporate networks going for $20,000 or more.

SMB incidents may grow as well: business email compromise (BEC) is a particular form of social engineering that uses the real accounts of company employees and

executives. The threat is particularly acute for companies that regularly transfer funds to vendors since the criminals (impersonating such vendors) ask the employees of the victim company to send funds to the criminals' own bank accounts. Such attacks have been reported widely and FBI estimates place damage in the last three years at $26 billion.

Government and politics

In the first three quarters of 2019, we recorded 167 attacks on government institutions (compared to 133 attacks in the equivalent 2018 period). As expected, attacks tended to involve phishing (49% of attacks) and malware (63% of attacks), although attacks on the websites of state-owned companies remain an ever-present hazard. In the first three quarters of 2019, 18 percent of attacks targeted web applications (nearly the same as in 2018, when the equivalent figure was 19%).

Attacker objectives include theft of personal data, defacement, and infection with cryptocurrency miners. Phishing and malware are used both to place ransomware and engage in espionage.

Forecasts

The political highlight of the current year is sure to be the 2020 U.S. presidential elections. One can expect high-profile cyberattacks to deface the sites of political parties and candidates. Attempts may be made to influence public opinion via social media. Nor can the possibility of attacks on e-voting systems be ruled out, considering the vulnerabilities that were shown in 2019.

Attacks on ordinary users

The number of attacks on individual users is growing. In the first three quarters of 2019, we identified 231 hacking campaigns targeting such users (compared to 217 in 2018). Usually these are mass attacks affecting a large number of victims simultaneously, making it impossible to calculate the exact scale or damages.

Unsurprisingly, social engineering and malware infection are the main methods for stealing user data. Criminals take advantage of poor security awareness among the public. Bruteforcing of passwords for sites and social networks was significant in 2018 (12% in Q1–Q3 2018) but has diminished in 2019 (6%). We believe this drop to be associated with support by the vast majority of services for two-factor authentication (2FA) and its widespread use in practice, making life more difficult for attackers.

Data theft attacks accounted for 64 percent of all attacks on individuals in Q3 2019. Almost half of such attacks aimed to obtain credentials for Internet services (47%), more than credit card numbers (23%), personal data (12%) or personal correspondence.

Attackers are actively making use of site vulnerabilities against ordinary people. Our statistics for 2019 show that 92 percent of web applications allow attacks on users. Of the vulnerabilities we found, 82 percent were caused by coding errors. On 16 percent of tested sites, it was possible to obtain control not only over the web application but the server as well. Such control enables serious attacks, such

as spreading malware or implanting JavaScript sniffers[1] in site code to steal credit card information. This trend has picked up in the past year in the e-commerce sector, but the global problem of web applications security remains as important as ever. As online retail continues its expected growth, such threats, including sniffers, are sure to keep pace.

"Dumps" of user information periodically appear on the darkweb, containing data stolen from different companies or negligently left out in the open online. It is hard to say whether this trend is specific to 2019, but this phenomenon certainly has become more publicized. Criminals can make significant profits by selling data whether in bulk or individually.[2]

Criminals can combine data from breaches over the last several years and sell the resulting compendium. No technical or hacking skills are necessary—they can simply go through past incidents at a particular company. Such incidents hit corporate reputation most of all. Minimizing the risks requires a comprehensive security approach encompassing employee security training, strict delineation of access rights, and deployment of field-oriented cybersecurity tools.

Forecasts

Attacks targeting site vulnerabilities, including JavaScript sniffers, will continue because they work. Ordinary users are powerless to improve the security of the websites where they shop and pay—this can be done only by the site owners. But users should pay close attention to the sites where they enter their credit card information: think twice before paying on an untrusted or little-known site. Larger and better-known companies are generally believed to have the best protection, but even big names have fallen victim and put their users at risk.

Data breaches will likely receive broader media coverage, especially in the case of breaches from market leaders.

The personal devices of users will continue to attract attackers, since convenience tends to prevail over the security of personal data. Attackers will likely try to combine attacks on phones and tablets with tried-and-true social engineering tricks (such as fraudulent phone calls to get bank information). With mobile devices being so embedded in our lives, they are a logical focus for those trying to steal data or bank deposits.

---

1. JavaScript sniffer is a small fragment of JavaScript code that attackers add invisibly to the legitimate code of a site. The sniffer steals the information entered by users. This is what happened in the infamous MageCart campaign, which had been known for several years but became more prominent in late 2018 and 2019. According to RiskIQ, 17.3 percent of all malware advertisements online offer such sniffers.

2. Our research shows that a single set of passport information costs approximately $2.

Dmitry Darensky
Head of Industrial Networks Security

Industrial sector at risk

Early 2019 saw several cyberattacks on major industrial companies. A cyberattack on aluminum producer Norsk Hydro forced the company to transfer processes to manual control and halt operations at some plants entirely after files at the company's plants and offices worldwide had been encrypted. Damage was estimated at $41 million. The ransomware used, LockerGoga, had also been detected in early 2019 in attacks on three chemical companies in the U.S. In June 2019, a different strain of ransomware struck aviation parts manufacturer ASCO, during recovery from which the company placed around 1,400 companies on unplanned leave.

Our research shows that in the first three quarters of 2019, 83 percent of attacks on industrial companies involved phishing and 89 percent involved malware. During the three quarters, we recorded 92 cyberattacks, substantially exceeding the prior-year figure for 2018 of 25. Mass attacks most often involve infection with cryptocurrency miners or ransomware. When attacking industrial and energy companies, the main objective is espionage: hackers burrow into infrastructure for as long as possible and obtain control over IT systems, key computers and servers, and even process networks containing industrial equipment.

Forecasts

Cyberespionage will not go away in 2020. Most attacks will build on previous successful attacks, and companies will learn to detect them. Awareness of cyberattacks and targeted APT attacks in particular has improved significantly. Companies are realizing the need to deploy effective systems that can both resist individual threats and detect the efforts of skilled hackers. Management of energy and industrial companies is truly starting to "get" the need for effective security processes.

Pavel Novikov
Lead Telecom Security Specialist

Insecure telecom

Vulnerabilities in 2G/3G networks remain a threat, enabling criminals to access subscribers' bank accounts. Flaws in mobile networks allow bypassing billing, charging services to other subscribers, intercepting SMS messages, eavesdropping on calls, and causing denial of service. The situation with 4G networks is little better: vulnerabilities make it possible to track subscriber location, bypass operator blocking of services, leave subscribers without communication, or downgrade subscribers to insecure 3G. Although operators encounter attacks every day, few have an understanding of how to respond.

The trend is that most "users" of mobile services will be not people, but things. A number of countries have already launched 5G test deployments, the main users of which are Internet of Things (IoT) devices. The security of telecom technologies has direct bearing on the security of smart IoT-based systems. We have found that it possible to deprive a subscriber of service no matter which network is in use, whether 2G, 3G, 4G, or even 5G. This currently means that smart home or industrial devices could be inaccessible at a critical moment. As 5G and the IoT spread, the threat surface will grow as well: victims could include smart cars or critical city infrastructure.

Forecasts

Deployment of 5G networks has entailed new risks due to wide use of virtualization, increased difficulty of administration, and use of Internet protocols that are old hat to today's hackers. What's more, real-world 5G networks currently rely on previous generations as part of the Non-Standalone architecture, built on top of 4G LTE. During the transition phase, devices connect to 5G frequencies when transferring data but still rely on 4G and 2G/3G for voice calls and SMS traffic. Accordingly, all the security issues in prior-generation networks will remain a threat to 5G subscribers for the foreseeable future.

Security issues in 2G/3G are unlikely to lose relevance anytime soon. Per the forecasts of the GSMA industry association, the number of users of 4G/5G networks is only starting to approach the number of 2G/3G users. No major drop in the number of 3G subscribers is expected until at least 2025, at which point 2G/3G users are still projected to make up a quarter of all users (not including IoT devices). The percentage of 4G users will only be growing until 2024 or later, while 5G networks rely on 4G infrastructure for the time being.

Securing the financial sector

Yaroslav Babin
Head of Banking Security

In the first three quarters of 2019, we recorded 61 attacks against financial companies (in Q1–Q3 2018, this number reached 69, and the total number of attacks for the whole year was 92). Phishing and malware were the main methods used by attackers to penetrate local networks of financial companies from the Internet. Phishing figured in 74 percent of cases and malware was used in 80 percent of attacks.

The slight decrease in the number of attacks against financial organizations can be explained in several ways. To begin with, we observed a significant fall in the number of mass attacks against financial companies. In Q3 2019, mass attacks accounted for only 4 percent of all cases, but in Q3 2018 they had been 32 percent. Most modern banks, especially large ones, can counter mass attacks (such as mailings containing ransomware), which forced hackers to focus on less protected sectors.

However, targeted attacks against financial institutions are not declining, as hackers keep updating their infrastructure and malware, target new regions, and select the most vulnerable victims.

In the first two quarters of the year, we saw attacks conducted by the Cobalt and Silence APT groups, as well as one more group that used network infrastructure similar to FinTeam. In the third quarter, Cobalt conducted attacks in Russia, Kazakhstan, and Europe. TA505 targeted European and African banks by sending phishing emails.

AI is finding a number of uses at financial institutions. Studies indicate a growing role for AI, and especially machine learning, in banking. ML both facilitates the use of banking services by end users and helps to prevent fraud.

POS terminals and ATMs

According to the non-commercial European Association for Secure Transactions (EAST), in the first two quarters of 2019, POS terminals were the primary victims of attacks against self-service payment systems in Europe (€124 million). Malware and black box attacks against ATMs[3] caused only slight damage, totaling less than €1,000.

Fraud with contactless payments is on the upswing, especially for transactions below the Cardholder Verification Method (CVM) limit, which do not require a PIN to confirm.

If 15 years ago the only providers of financial services were banks, acquirers, and payment systems such as Visa and MasterCard, today many more entities have access to cards and banking information: Apple Pay and Samsung Pay, manufacturers of mPOS terminals and smartphones, and mobile operators. As the number of parties with direct and indirect access to banking accounts and cardholder information grows, so does the risk of a data breach and fraud. The same applies to online banking.

In 2018, the PSD2 Payment Services Directive came into force in the European Union. The directive is intended to advance innovation in the financial sector and

3. Attack performed by connecting a third-party device directly to the cash dispenser of an ATM.

create a more secure space for customers. Among the mandates of PSD2 are the following:

- **Banks must provide open APIs to all third-party providers of financial services.**
- **Strong Customer Authentication requires that authentication be multifactor, such as periodically checking for two out of three factors (these could be PIN, fingerprint, facial recognition, etc.). Under SCA, customers will have to insert their cards into the reader after each five contactless transactions, and mobile applications will periodically ask for the PIN even if fingerprint authorization is enabled.**

Systematic implementation of such measures is the key to making banking systems more secure, especially when it comes to the delicate question of contactless card payments.

Forecasts

Criminals will build on their success with phishing and malware to penetrate bank networks. However, malefactors will need to modify and camouflage their malicious code in order to sneak through defenses. They will keep using newly published exploits to conduct attacks within just hours of publication, to catch targets before they have updated. Exploits for zero-day vulnerabilities are expensive on the darkweb and, mindful of the dent to their earnings, hackers will not spring for them often. Moreover, banks take a long time to roll out updates and may harbor known vulnerabilities for which security patches have already been released (such as CVE-2017-11882 in Microsoft Office). Even now, hackers can successfully exploit these vulnerabilities at banks without having to spend money on expensive zero-days.

Mobile banking is popular, which means that hackers will likely focus on attacking mobile bank applications. Criminals will likely seek out vulnerabilities related to user data disclosure. We expect to hear of breaches of personal data, including credit card numbers. We also expect an increase in unimaginative social engineering attempts, such as fake SMS messages and phone calls from banks. Unfortunately, such methods still remain the most effective ones due to low user security awareness.

AI will grow in the finance sector, contributing to cybersecurity and antifraud efforts. All this suggests that criminals will invent new ways to commit online banking fraud, or else move on to easier pickings such as online stores and ticket sellers.

Hardware vulnerabilities

Dmitry Sklyarov
Head of Reverse Engineering

Mark Ermolov
Lead Specialist of OS and Hardware Security

Hardware vulnerabilities are a true blast from the past. Foremost among them are the Meltdown and Spectre processor vulnerabilities, Intel ME and Intel VISA security flaws, and other vulnerabilities that have started to appear at security conferences with increased frequency.

Many hardware vulnerabilities discussed today by researchers all over the world are the consequence of dubious decisions stemming from manufacturers' desire to boost performance or ease software development.

Side-channel attacks

Originally created in the 1980s, the x86 processor architecture—in particular, its system for controlling access to CPU resources—allows attackers to exploit speculative execution vulnerabilities that bypass current protections.

The Spectre and Meltdown speculative execution vulnerabilities allow attackers to extract critical data to which unprivileged code should not have access, by using the CPU cache as a side channel with the help of special techniques such as FLUSH+RELOAD. The Spectre and Meltdown vulnerabilities were discovered by a Google researcher (as part of Project Zero) and by researchers at the Graz University of Technology (Austria) in 2017, respectively.

These vulnerabilities affect most modern Intel and AMD processors and some ARM processors.

Attacks can exploit these vulnerabilities to bypass hardware security and, in shared computing environments, obtain access to cloud data of other users on remote servers.

Of course, this is not the result of anyone purposefully inserting a backdoor into the architecture. Rather, a combination of mistakes and questionable decisions have contributed to this state of affairs.

Hardware reverse engineering

Over the last two years, we have seen only the tip of the iceberg of hardware vulnerabilities. Searching for vulnerabilities has become quite a trend among researchers who, while hunting for flaws in hardware, descend ever deeper into the technical depths and (somehow!) find vulnerabilities even at the level of board components and hardware logic.

Experts are moving in the direction of hardware reverse engineering: see how pictures of CPU cores taken with electronic microscopes keep appearing online. Previously, probing CPU security was the realm of amateurs and a very niche interest. With today's greater amount of knowledge, engaged researcher community, and broad media coverage, hardware vulnerabilities should be viewed as a serious threat

Changing the threat model

For end users, such attacks are more theoretical than threatening. Hardware exploitation remains too complicated and expensive, so the bill has not come due yet.

Business, though, should take such threats seriously, understand the risks, and prepare to counteract possible attacks. There has been no significant damage so far,

but the problem needs to be addressed. Large companies seem to be well aware of it as they include such vulnerabilities in their threat models, allocate budgets, and invest in the development of security mechanisms and personnel training. These substantial sums go towards patching up the "gaps from the past" mentioned previously. Sources of office dangers are more than just computers: vulnerabilities are being found in routers, servers, printers, and mobile devices.

Data breaches are painful for regular users, but can also bring companies and governments to a halt, as well as disrupt infrastructure and healthcare.

CPU manufacturers are working together with researchers and major software vendors to fix the mistakes that gave rise to such vulnerabilities. Manufacturers are acknowledging security flaws and mitigating vulnerabilities in their latest processors. That said, the problem is so extensive that a solution is still far off, leaving business and infrastructure at increased risk.

Nikolay Anisenya
Head of Mobile Application Security

Mobile threats

Today, more than half of the world population has smartphones. Massive uptake of mobile devices has spurred criminals to add to their toolkit. Attack vectors include rooting and jailbreaking (such as checkm8), bypassing biometrics, evading pinning,[4] abusing lack of code protection, and attacking users.

Bypassing biometrics

Tencent Security's X-Lab team demonstrated how to break into a smartphone in just 20 minutes by using fingerprints on a drinking glass. They managed to recreate a fingerprint with the help of the Tencent Security application, which can clone fingerprints from fragments taken from multiple objects, plus an engraving machine costing $140.

Most mobile bank applications use biometric authentication with fingerprint or facial recognition. However, this simplifies authentication for malefactors too. The application stores authentication data on the device. Although users can log in with their username and password, the simplicity of authentication by PIN or biometrics often outweighs security concerns. Our experience shows that 25 percent of applications allow hackers to bruteforce PIN codes locally, and five out of eight apps verify PIN codes locally.

One attack scenario may look as follows. An attacker with access to an unlocked device may try bruteforcing a bank application PIN code if the device does not block PIN bruteforcing or does so incorrectly. In most cases, attackers will need no more than 10,000 attempts to gain access to banking data. By manually bruteforcing PIN codes, attackers can obtain the needed information in hours. Obtaining an unlocked mobile phone is as simple as snatching it from the victim's hand.

Lack of code protection

Rooting and jailbreaking pose a serious security risk. Yet developers still pay little attention to protecting mobile applications from such attacks. Two thirds of applications that we analyzed in 2019 continued to run even when users had obtained root or jailbreak rights, or did not warn customers about the danger of using such configurations. None of these applications contained any signs of obfuscation sufficient to prevent code analysis. This plays into attackers' hands, as malicious applications can easily exploit escalated privileges.

User attacks

User-installed malicious applications remain the most common vector against mobile phone users. These applications ask for permissions to administer the device, appear on top of other windows, enable accessibility services (intended for users with disabilities), and share the screen. In some cases, however, no special permissions are required. One example is a vulnerability in Android WebView discovered by a Positive Technologies expert.

4. Certificate pinning refers to incorporating a certificate needed for establishing a secure connection in the code of the application itself. This helps protect against attacks aimed at spoofing certificates. Even if the user has installed a malicious certificate as trusted, no connection will occur and data will not be transferred, leaving the user in safety.

WhatsApp vulnerabilities

Highly publicized vulnerabilities in WhatsApp prove that even a thoroughly checked application may still contain remotely exploitable vulnerabilities. Researchers also observed a new trend of attacks that take advantage of media files such as videos and images.

As we expected last year, the evolution of mobile phones has not gone unnoticed by criminals: smartphone attacks involving remote access applications are more and more frequently covered in the media. Hackers can use remote access to obtain a mobile banking password or perform actions impersonating the user.

In 2019, Google took a major step towards improving the security of popular Google Play mobile applications. Under the Google Play Security Rewards Program, security researchers can receive rewards for identifying vulnerabilities in any Android application installed more than 100 million times. This will likely improve the security of popular Android applications.

Operating Systems Security

Alexander Popov
Lead Researcher,
Operating Systems
Security Team

Operating systems security has undergone notable changes in recent years. It all started when OS developers realized that it is impossible to fix each and every mistake in code. As OS code becomes increasingly complicated, new mistakes appear faster than old ones get fixed. Moreover, some of these mistakes cause security vulnerabilities. In order to improve the security of operating systems, two complementary approaches have been put to use.

The first approach: develop OS kernel self-protection mechanisms. In case of an error or attack, the system should resolve the problem safely itself. These mechanisms should protect the system against whole classes of errors. One popular metaphor compares the development of today's operating systems with the automobile industry of the 1960s. At that time, high crash injury rates forced manufacturers to prioritize passenger safety for protection in case of an accident. Similar technologies are being developed for operating systems now. In 2019, the Microsoft Security Response Center published a detailed overview of the types of Windows kernel vulnerabilities and methods to mitigate them. There is also a Linux Kernel Defence Map developed by Alexander Popov that shows the relationships between vulnerability classes, exploitation techniques, and protection mechanisms in the Linux kernel.

However, practice shows that self-protection mechanisms in the operating system kernel come at a price. Reduced performance and difficulties for system developers are two of the results. Attempts to fix the Spectre, Meltdown, and MDS hardware vulnerabilities at the OS level testify to this.

The second approach involves continuous use of automated dynamic and static analysis. Operating systems are generally written in low-level programming languages. These languages are powerful, while requiring plenty of care and skill from the developers. However, people make mistakes, which is where automated testing tools come to the rescue. This approach includes different methods of static analysis including pattern-based vulnerability discovery, and dynamic analysis technologies, the most popular of which is fuzzing (testing software by using random inputs). The syzkaller fuzzer is one notable example of a project that has contributed greatly to the code quality and security of operating systems.

However automated vulnerability discovery tools also have their downside, since their findings can be useful to both defenders and attackers.

Conclusion

"Security debt" has accumulated, giving reason for major concern. Although hardware vulnerabilities have not yet caused significant damage, clear-sighted companies have started to include them in threat models realizing that when criminals learn how to exploit such vulnerabilities, it will be too late to stay safe.

APT attacks ran rampant in 2019, threatening businesses, governments, and infrastructure.

The law of unintended consequences is alive and well in the technology world. The imminent uptake of 5G networks means new risks for telecom operators. Artificial intelligence and machine learning make life easier, but at the same time aid attackers greatly in improving their toolkit, including new social engineering methods.

Technologies are integrating and transforming, giving rise to a range of novel attack vectors. Security professionals are faced with urgently counteracting threats and adapting to the current needs of corporate and individual clients. Meeting this challenge will require a resolute and fundamentally new approach to cybersecurity.

ptsecurity.com
info@ptsecurity.com

Cybersecurity-2019-2020_A4.ENG.0003.01