Kaspersky ICS CERT

kaspersky

Biometric data processing and storage system threats

Kirill Kruglov

02.12.2019 Version 1.0

Contents

Initially, digital biometric data processing systems were used primarily by government agencies and special services (police, customs, etc.). However, the rapid evolution of information technology has made biometric systems accessible for ‘civil’ use. They are increasingly becoming part of our everyday lives, augmenting and replacing traditional authentication methods, such as those based on logins and passwords. Indeed, identifying people using characteristics that are unique to each person, such as fingerprints, voices, facial shapes or their distinctive eye structure, seems an obvious and incredibly convenient method.

Today, biometric authentication is used to access government and commercial offices, industrial automation systems, corporate and personal laptops and mobile phones. Both the number and the variety of applications for these technologies continues to grow.

Unfortunately, like many other technologies that have been rapidly evolving lately, biometric authentication systems have proved to have significant drawbacks. The key shortcomings of biometric authentication technologies have to do with information security issues.

In this report, we will discuss the numerous information security issues affecting biometric authentication systems and present the results of our own research, to provide additional information for a more objective evaluation of risks associated with using existing biometric authentication system implementations.

Biometric data processing and storage

The concept of biometric data as a unique personal identifier that cannot be forged is fundamentally wrong and can foster a false sense of security.

Firstly, the accuracy of biometric data recognition by authentication systems, although relatively high, can still be insufficient for many applications. After all, such recognition is not about simply calculating whether two hash sums are equal or not, as in the case of password-based authentication. Biometric systems usually have a greater-than-zero probability of false-negative and false-positive results.

Secondly, research demonstrates that many human biometric characteristics can be forged (falsified) by malicious actors, and copying digitized biometric data may be even easier than copying physical biometrics.

Thirdly (and most importantly), biometric data, once compromised, is compromised for good: users cannot change their stolen fingerprints the way they do stolen passwords. What's more, biometric data may turn out to be compromised for all applications at the same time. An individual will therefore potentially be affected for the rest of his or her life.

Given all of the issues above, it is remarkable how careless biometric authentication system developers and users are about protecting these systems and the biometric data collected by them against computer attacks.

It turns out that biometric data may be stored in a format that is easily accessible to attackers. A striking example is the notorious story of a major breach found in BioStar 2, a web-based biometric security smart lock platform. According to researchers, the service had a publicly accessible database - over 27.8 million records, a total of 23 gigabytes of data on employees within 5,700 organizations, from 83 countries. The database contained, among other confidential data, about one million fingerprint records, as well as facial recognition information. According to the report, "…instead of saving a hash of the fingerprint (that can't be reverse-engineered) they are saving people's actual fingerprints that can be copied for malicious purposes."

Unfortunately, the problem pointed out by researchers in connection with the BioStar 2 story is by no means far-fetched. There are known cases of biometric data being targeted by attackers. For example, information stolen in a 2015 cyberattack included nearly six million fingerprints of people associated with the US government.

As the number of potential applications for biometric authentication systems grows, it could easily be envisaged that biometric data will be of interest not only to special services (which the Office of Personnel Management believes is most likely to have been behind their 2015 attack), but other categories of attackers, as well.

Threats blocked on biometric data processing and storage systems

With the risks described above in mind, we decided to evaluate to what extent biometric data processing systems (servers that process and store data, as well as workstations used to collect biometric data) are open to malware attacks, so we analyzed the threats blocked by Kaspersky products on such systems.

Research focus

Computers (servers and workstations) used to collect, process and store biometric data (such as fingerprints, hand geometry, face, voice and iris templates) on which Kaspersky products are installed.

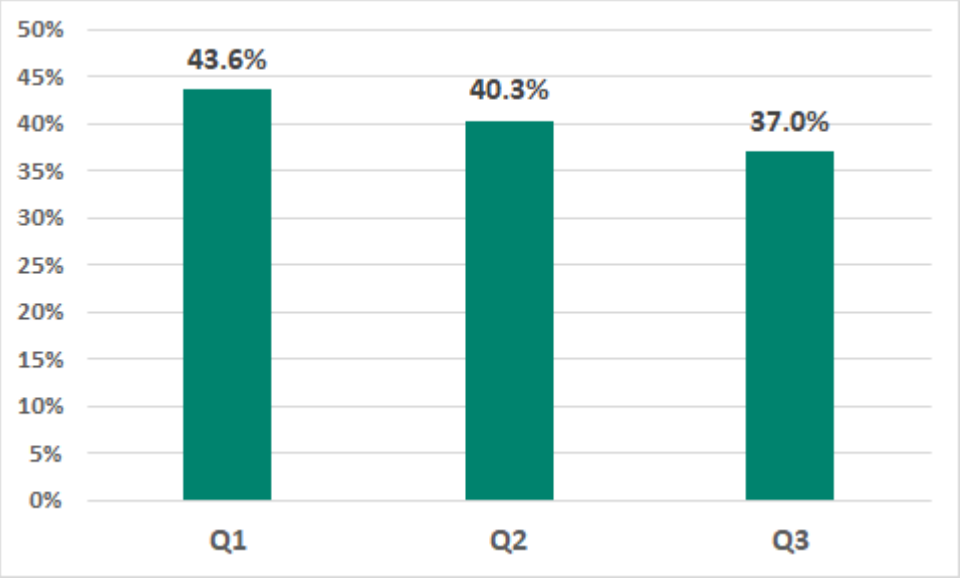
Reporting period

Q3 2019.

One third of systems under threat

According to Kaspersky Security Network (KSN) data, in Q3 2019 malware was blocked on 37% of computers that perform the functions of collecting, processing and storing biometric data – in other words, one computer in three was at risk of malware infection.

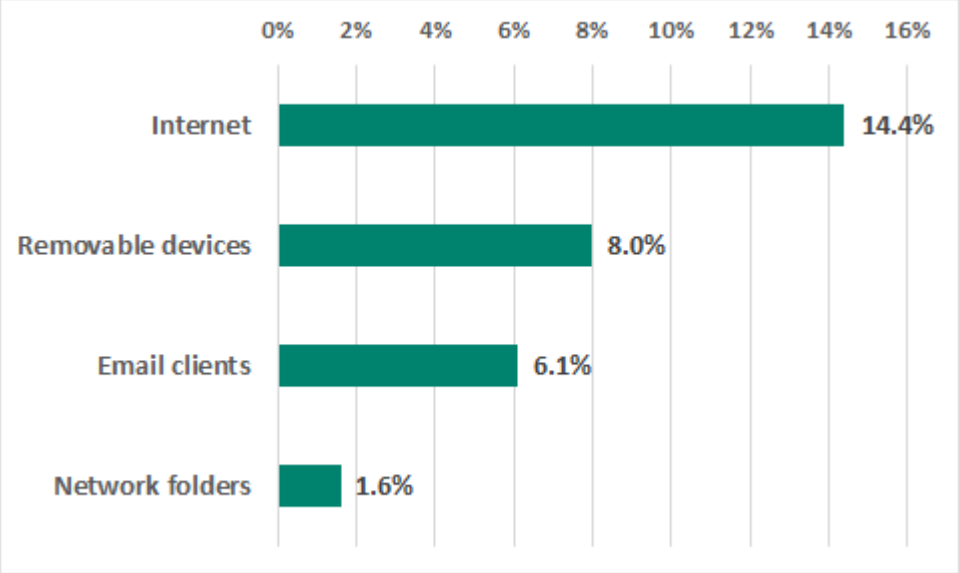
It can be seen in the quarterly data below that although the percentage of computers on which malware was blocked has decreased by 6.6 percentage points since the beginning of 2019, it remains at a sufficiently high level.



Percemtage of biometric processing system computers on which malware was blocked, Q1 – Q3 2019

Threat sources

An analysis of threat sources has shown that, as with many other systems that require heightened security measures (such as industrial automation systems, building management systems, etc.), the internet is the main source of threats for biometric data processing systems.



Main sources of threats for biometric data processing and storage systems, Q3 2019

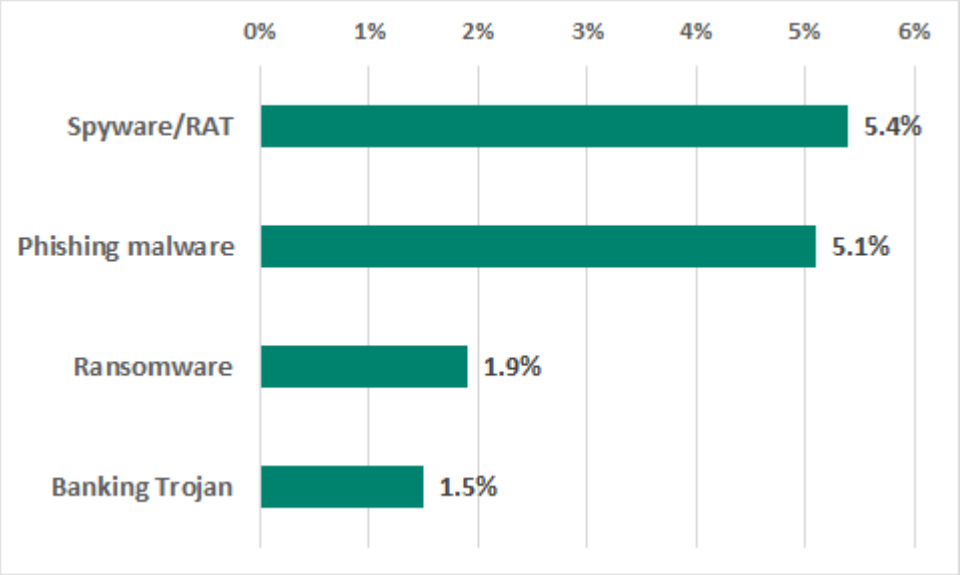
Internet-borne threats were blocked on 14.4% of all biometric data processing systems. This category includes threats blocked on malicious and phishing websites, as well as web-based email services.

Removable media (8%) and network folders (6.1%) are most often used to distribute worms. After infecting a computer, worms commonly download spyware and remote access Trojans, as well as ransomware.

As for threats blocked in email clients, in most cases these were typical phishing emails (fake messages on the delivery of goods and services, the payment of invoices, RFQ, RFP, etc.) containing links to malicious websites or attached office documents with embedded malicious code.

Most dangerous

Among the threats blocked on biometric data processing and storage systems, we highlighted spyware, malware used in phishing attacks (mostly spyware downloaders and droppers), ransomware, and banking Trojans as posing the greatest danger to such systems.



Some of the malware types blocked on biometric data processing and storage systems

Overall, in Q3 2019 spyware was blocked on 5.4% of computers used to collect, process and store biometric data. Malware used in phishing attacks and ransomware was blocked on 5.1% and 1.9% of such computers, respectively.

It should be noted that other types of malware also included malicious programs designed to steal banking data (1.5%). It is not likely that these malicious programs were intended for stealing biometric data. However, it can be expected that mass-distributed malware designed to steal biometric data from banks and financial systems will appear in the near future.

Conclusion

As discussed above, in Q3 2019 37% of computers used to collect, process and store biometric data were at risk of malware infection. Among other malicious objects, Kaspersky products blocked modern remote-access Trojans (5.4% of all computers analyzed), malware used in phishing attacks (5.1%), ransomware (1.9%), and Trojan bankers (1.5%).

Although malware blocked on the computers analyzed is not specific to biometric data processing systems, the danger posed by it should not be underestimated.

Such malware is capable of:

- stealing confidential information;
- loading and executing arbitrary software;
- enabling attackers to control infected computers remotely.

Although such threats are not specifically designed to steal biometric data or tamper with it, some of them have the technical capability to do that. In addition, the side effects of an active infection could significantly affect the availability of authentication systems and the integrity of biometric data.

This is why we believe that exposing biometric systems to random cyberthreats is a huge risk for both the service provider and the people who have entrusted their biometric data to it.

It should also be noted that, as we determined in the course of our research, biometric data processing and storage systems (and specifically biometric databases) are often deployed on application servers shared with other systems, rather than dedicated computers. In other words, if attackers compromise, say, a mail server or a database used by the website of an organization that has a biometric authentication system, the chances are that they will also find the biometric database on the same server.

Given all of the above, we believe that the existing situation with the security of biometric data is critical and needs to be brought to the attention of industry and government regulators and the community of information security experts, as well as the general public. After all, anyone can be at risk in this case, regardless of their occupation, professional background and skills.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com