The infamous Prilex threat actor sells new dangerous and sophisticated PoS malware across the globe

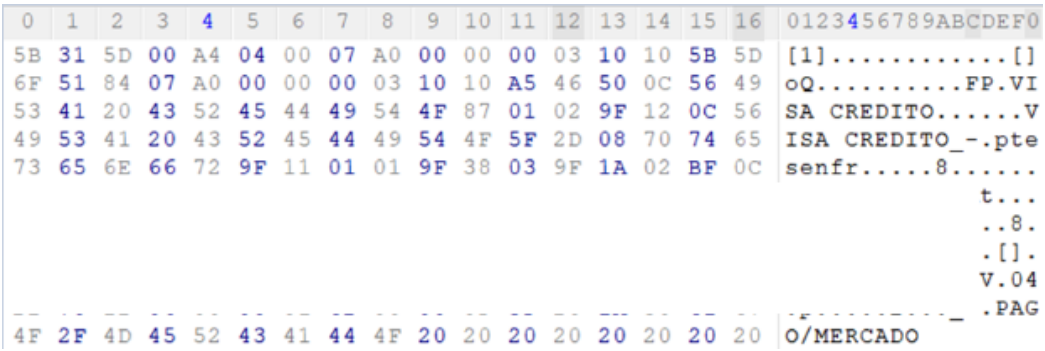
Kaspersky ⋮ 8-10 minutes ⋮ 9/22/2022

Prilex is a well-known and dangerous threat actor, targeting the core of the payment industry – Automated Teller Machines (ATMs) and Point of Sales (PoS) terminals. Active since 2014, Prilex was allegedly behind one of the largest attacks on ATMs in Brazil. During carnival in 2016, the actor cloned over 28,000 credit cards and drained more than 1,000 ATMs in one of the Brazilian banks. The fraudsters stole all funds present in the machines, and the damage after this incident was estimated at millions of dollars.

In 2016, the group focused all their attacks on PoS systems only. Since then, cybercriminals have greatly improved their malware, making it a complex threat that evolves quickly, having a major impact on the payment chain. Now Prilex threat actor conducts so-called “GHOST” attacks – fraudulent transactions using cryptograms – previously generated by the victim’s card during the store payment process.

The initial machine infections are usually delivered through social engineering. After choosing a target, cybercriminals call the business owner or their employees and say their PoS software needs to be updated by a technician. Later, the fake technician comes to the targeted company in person and infects the machines with malicious software. In another scenario, fraudsters request the target to install AnyDesk and provide access to the fake technician in order to install the malware remotely.

Prior to striking victims, cybercriminals perform an initial screening of the machine, in order to check the number of transactions that have already taken place and whether this target is worth attacking. If so, the malware will then capture any running transaction and modify its content in order to be able to capture the card information. All the captured card details are then saved to an encrypted file, which will be later sent to the attackers’ server, allowing them to make transactions through a fraudulent PoS device registered in the name of a fake company.



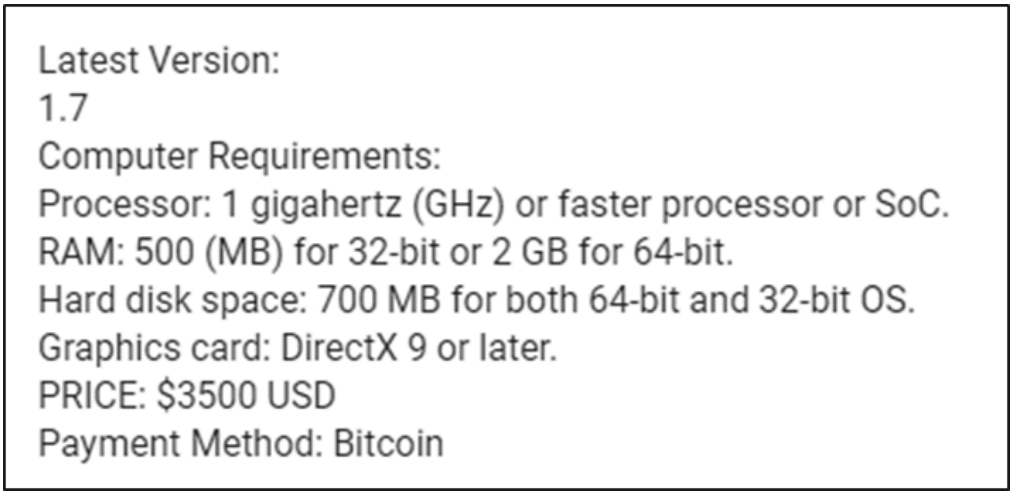
Captured credit card data that will be later sent to the operator server

Thus, having attacked one PoS system, attackers obtain data from dozens and even hundreds of cards daily. It is especially dangerous if the infected machines are located in popular shopping malls in densely populated cities, where the daily flow of customers can reach thousands of people.

In the recent investigation, Kaspersky experts have also uncovered that the Prilex group is controlling the development lifecycle of their malware using Subversion, used by professional development teams. Also, a supposed official Prilex website are selling the kits of their malware to other cybercriminals as Malware-as-a-Service. Prilex has previously sold various versions of its malware on the darknet, for example, in 2019 a German bank lost more than €1.5 million in a similar attack by the Prilex malware. Now, with the emergence of their MasS operation, highly sophisticated and

dangerous versions of PoS malware could spread to many countries, and the risk of losing millions of dollars would increase for businesses all around the world.

Kaspersky researchers also discovered websites and Telegram chats where cybercriminals sell Prilex malware. Posing as the Prilex group itself, they offer the latest versions of PoS malware, costing from $3,500 to $13,000. Kaspersky experts are not confident about the real ownership of these websites, as they can be copycats, trying to impersonate the group and steal money using its recent fame.



Cybercriminals ask $3,500 USD for the supposed Prilex PoS kit

"In movies we often see how robbers break into a bank with a gun in their hands, drain the till and flee the scene, taking a huge bag of money with them. In the real world, however, bank robberies take place quite differently. Nowadays real criminals are very stealthy: they usually attack remotely using malware without any physical contact with the bank. This makes them much harder to detect, and until ATM and PoS are sufficiently protected and updated, the number of threats and incidents will only increase," comments Fabio Assolini, head of the Latin American Global Research and Analysis Team (GReAT) at Kaspersky.

The Prilex family is detected on all Kaspersky products as ***HEUR:Trojan.Win32.Prilex*** *and* ***HEUR:Trojan.Win64.Prilex***

Read more about Prilex in the full report on Securelist.

To protect yourself from Prilex, Kaspersky recommends:

- **Use a multi-layered solution**, offering an optimal selection of protective layers to provide the best security level possible for devices of differing power and with different implementation scenarios
- **Implement self-protection techniques** into PoS modules, such as the protection available on our Kaspersky SDK, aiming to prevent malicious code from tampering with the transactions managed by those modules.
- **Secure older systems with up-to-date protection.** Solutions should be optimized to run with full functionality on the older versions of Windows as well on the newest Windows families. This ensures the business that it will be provided with total support for the older families for the foreseeable future, and gives it an opportunity to upgrade anytime it is needed.
- **Install a security solution** that protects devices from different attack vectors, such as Kaspersky Embedded Systems Security. If the device has extremely low system specs, the Kaspersky solution would still protect it with a Default Deny scenario.
- For financial institutions that are victims of this kind of fraud, Kaspersky recommends the Threat Attribution Engine to help IR teams to **find and detect Prilex files** in attacked environments.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

The infamous Prilex threat actor sells new dangerous and sophisticated PoS malware across the globe

Kaspersky researchers have discovered that the Prilex threat group, famous for stealing millions of dollars from banks, has evolved substantially. After developing both its technical innovations and marketing and business strategies, Prilex has upgraded its tools from a simple memory scraper to an advanced and complex malware, that now targets modular Point of Sales (PoS) terminals. Cybercriminals are also actively selling their malware on the darknet as Malware-as-a-Service, which means it is now available to other fraudsters, and the risk of losing money is increasing for businesses all around the world.

kaspersky