ATM/PoS malware “recovers” from covid-19, with the number of attacks continuing to grow in 2022

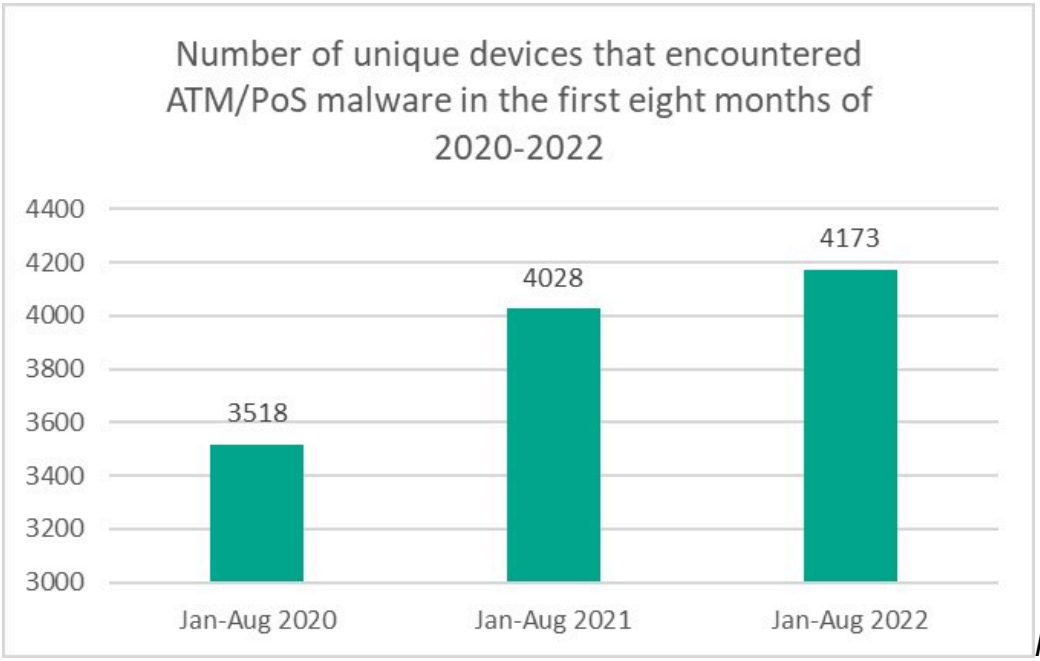
Kaspersky ⋮ 7-9 minutes ⋮ 10/5/2022

Cybercriminals attack embedded systems used in ATMs and point-of-sale (PoS) terminals to steal cash, credit card credentials and personal data, and penetrate systems to gain control over all devices within a network, and attackers can obtain thousands of dollars overnight. Many Windows versions used in ATMs reached the end of their support long ago and may be an easy target, while PoS terminals are used by many businesses with a low cybersecurity maturity level.

A look at the numbers: attackers’ activity returning to pre-pandemic levels

When the pandemic hit, the number of attacks decreased sharply compared to the previous year – from roughly 8000 in 2019 to 5000 in 2020. According to the experts’ assessment, this occurred for several reasons – including a reduction in the total number of ATMs across the world, their shutdown during pandemic restrictions, as well as people’s spending shrinking overall. As a consequence, attackers saw their market contract in terms of the number of their targets.

Today the restrictions have softened greatly, old spending patterns are back, and therefore threat actors’ activity is gathering pace. In 2021, the number of devices encountered with ATM/PoS malware was up by 39% compared to the previous year. In the first eight months of 2022, the number grew by 19% compared to the same period of 2020, and by nearly 4% compared to 2021. In total, 4173 devices were attacked in January-August of 2022.



Number of unique devices that encountered ATM/PoS malware in the first halves of 2020-2022

Given this trend, experts expect the number of attacks on ATM/PoS devices to increase further in the fourth quarter of 2022.

PoS malware is the most widespread

HydraPoS and AbaddonPoS account for roughly 71% of all ATM/PoS malware detections in 2020-2022, with 36% and 35%, respectively. The leader of the rating, HydraPoS, originates from Brazil and is known for cloning credit cards. According to Kaspersky Threat Intelligence Portal reports, this

family was used in attacks involving social engineering. "*There are different techniques. They depend on who is conducting the attack and which family is used. Attackers make phone calls or even come to victims' offices. They impersonate an employee of a bank or credit card company and try to convince the victim to install malware as if it were a system update*", comments Fabio Assolini, Head of Research Center, Latin America at Kaspersky.

№	Family	Share by detections
1	HydraPoS	36%
2	AbaddonPoS	35%
3	Ploutus	3%
4	RawPoS	2%
5	Prilex	2%

The most active ATM/PoS malware families in 2022 by share of detections

The TOP-5 also includes Ploutus (3%) – the malware family used for modifying legitimate software and privilege escalation to control ATMs and obtain administrative privileges that allow criminals to jackpot ATMs on demand. RawPoS (the malware able to extract the full magnetic stripe data from volatile memory) and Prilex (the malware abusing processes related to PoS software and credit and debit card transactions), account for 2% per each. The other 61 analyzed families and modifications account for less than 2% per each.

"PoS malware is more widespread than ATM malware because it gives fairly easy access to money. If ATMs are usually protected well enough, the owners of cafes, restaurants, and shops often don't even think about the cybersecurity of their payment terminals. This makes them a target for attackers. Moreover, new criminal business models like malware-as-a-service emerge to lower the skills bar for would-be threat actors," elaborates Fabio Assolini.

To read the full ATM/PoS malware report, please visit Securelist.com. In order to keep embedded systems and data safe, Kaspersky researchers recommend implementing the following measures:

- In order to keep embedded systems and data safe, Kaspersky researchers recommend implementing the following measures:
- Use a multi-layered solution providing an optimal selection of protective layers to give the best security level possible for devices of differing power and with different implementation scenarios.
- Implement self-protection techniques in PoS modules, such as the protection available in our Kaspersky SDK, aiming to prevent malicious code from tampering with the transactions managed by those modules.
- Protect older systems with up-to-date protection. Solutions should be optimized to run with full functionality on older versions of Windows as well the newest Windows families. This lets the business be sure it will be provided with total support for the older families for the foreseeable future, and have an opportunity to upgrade anytime it's 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 will 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 find and detect ATM and PoS threats in attacked environments.
- Provide your team with access to the latest threat intelligence (TI). The Kaspersky Threat Intelligence Portal is a single point of access for the company's TI, providing cyberattack data and insights gathered by Kaspersky over the past 20 years. To help businesses enable effective defenses in these turbulent times, Kaspersky has announced free access to independent,

continuously updated, and globally sourced information on ongoing cyberattacks and threats. Request access here.

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 to them most. Learn more at www.kaspersky.com.

ATM/PoS malware "recovers" from covid-19, with the number of attacks continuing to grow in 2022

In 2020, the number of attacks on ATMs and PoS terminals significantly decreased due to the pandemic. Now, with old spending patterns back, threat actors' activity is on the up again. HydraPoS and AbaddonPoS are the most widespread malware families in 2022, accounting for roughly 71% of all detections. For ATMs the most active malware is Ploutus, accounting for 3% of all detections in the first eight months of 2022. These and other findings are part of a new ATM/PoS malware report issued by Kaspersky.

kaspersky