SOLUTION BRIEF

PROTECTING POINT-OF-SALE SYSTEMS

With their highly valuable payment card and personal sensitive information, Point-of-Sale (POS) systems present a ripe target for cybercrime groups. A successful breach can have enormous consequences for the attacked organization, from detecting and responding, to notifying victims, post-response support, lost business and potentially hefty government fines.

Modern POS environments are complicated systems with multiple entry points for attack, from phishing emails or drive-by-download exploits on employee computers to vulnerable third-party suppliers. And while payment card security standards have introduced a basic protection framework, POS-attacks have not abated under the regulations — some of the largest breaches of the past several years are due to POS attacks.

MORPHISEC FOR POS

- Prevents unknown threats, exploits, fileless attacks, zero-days and evasive malware
- Virtually patches vulnerabilities
- Extremely lightweight 2MB agent; no updates, scans or any interference with continuous availability
- Windows 7 compensating control for PCI compliance
- Stops lateral movement across networks
- Functions seamlessly across virtual, physical or hybrid IT environments

MORPHISEC
Moving Target Defense

POINT-OF-SALE AS POINT OF COMPROMISE

POS systems are a weak security point for most networks. They are in constant use and often are not patched or updated — sometimes containing legacy systems that can't be patched at all. Vendors and other third parties may have access to the systems, adding another level of risk.

POS systems also can be difficult to secure with anything but the most basic protection tools as many security products are resource-intensive, slow down performance and interfere with continuous availability. Today's advanced attacks use multiple techniques to avoid detection — such as hijacking legitimate system resources to perform malicious actions — and can easily bypass traditional POS defenses.

An Increasing Target

POS systems have not only become a target of choice for notorious cybercrime groups like FIN6, Carbanak/FIN7 and FIN8, but POS malware kits can be purchased on the cybercrime underground so even those without skills and infrastructure can set up shop. In fact, nearly 90% of cyberattacks on the accommodations and restaurant industries involve POS intrusions.

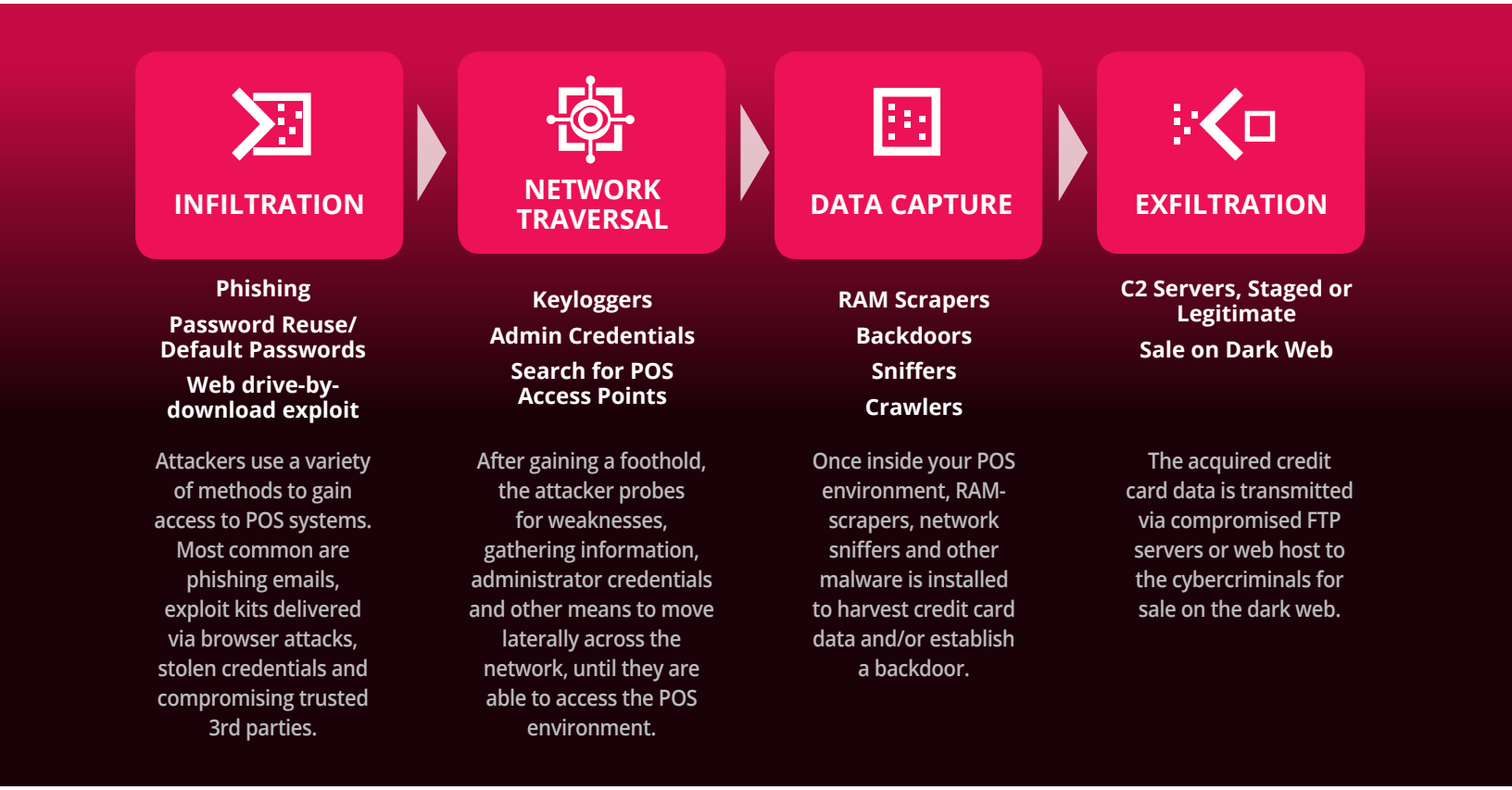
POS malware is really a generic term for the expanding number of memory-scraper Trojans that are designed to scan for, grab and exfiltrate credit and debit card data from the endpoints that process and store it. Cybercriminals easily cash in this valuable information through dark web markets. In addition, POS systems serve as gateways where attackers can enter and move laterally to an organization's regional, national or global data systems.

PCI Compliance — Necessary but not Sufficient

PCI DSS compliance is compulsory for any organization handling cardholder data. This applies to all parts of the cardholder data environment (CDE), including POS systems. Failure to adhere can mean regulatory fines and fees, increased audits and more. However, PCI compliance does not mean that card data is secure. PCI regulations stipulate that CDE environments be protected by firewalls and antivirus, but advanced POS attacks are engineered to evade these solutions. Security teams need to consider additional steps and technologies to really reduce risk and prevent the possibility of brand-damaging breaches. With GDPR now in effect, the need is even more acute as data privacy violations can mean big fines and strict notification and mitigation planning requirements. With stakes this high, early attack prevention is critical. If an attack is stopped before it can enter the system, then notification and remediation become a moot point.

Anatomy of a Point-of-Sale Attack

Cybercriminals have developed sophisticated multi-stage attack methodologies to target valuable cardholder data. An attack generally includes the following phases:



TRADITIONAL POS PROTECTION APPROACHES

In addition to encryption technology, password policies and other security procedures, organizations usually rely on a combination of network segmentation (firewalls) and antivirus to protect their POS environment.

Firewalls / Network Segmentation

A basic PCI requirement is installing a firewall and segmenting POS components from the rest of the network. Firewalls filter traffic and block potential threats, for example by matching an IP address against a black-list or reputation feed. They are effective at defending against known threats both within and at the perimeter of your network, but new attack techniques allow some to go undetected for minutes, days, even months. Fileless threats that attack via legitimate applications also pose a problem for firewalls as highly restrictive policies that might catch such threats can negatively impact daily business operations.

Antivirus

POS terminals and servers are also generally protected with antivirus / anti-malware, which is important for preventing basic attacks, but offers limited protection from advanced threats. Both traditional antivirus and NGAV solutions detect or predict malicious activity based on signatures, heuristics or other indicators. This means they are ineffective against new, unknown threats and highly evasive attacks. They also require a heavy database of known signatures and constant updates for newly identified attacks, which slow down POS terminals. Many businesses update sporadically, if at all, leaving them dangerously exposed.

MORPHISEC FOR POINT-OF-SALE SYSTEMS

Traditional POS protection methods leave serious gaps that place your business and customers at risk. However, loading up slim POS terminals with additional security layers that require resource-intensive monitoring or constant connectivity is simply not feasible from a system performance point of view.

The Morphisec Unified Threat Prevention platform uses powerful, patented Moving Target Defense technology to prevent attacks on POS endpoints, thin clients and servers immediately, before they infiltrate your environment. Morphisec can be deployed rapidly and requires almost no management; with an extremely lightweight agent that does not slow performance, need updating or otherwise disrupt your ongoing business.

Prevents Advanced Unknown Threats Instantaneously

The most dangerous threats to POS systems are targeted attacks engineered to bypass security tools. They use fileless techniques to operate in memory, leveraging legitimate system resources and constantly changing their methods so that they do not trigger detection tools. Morphisec's unique Moving Target Defense technology makes it impossible for these types of attacks to execute, immediately preventing and neutralizing them.

Virtually Patches Vulnerabilities

According to a Ponemon study, nearly 60% of data breaches were caused by exploiting a software vulnerability that was known, but which the victim organization had not yet patched . Morphisec prevents attacks on unpatched operating system and application vulnerabilities. Morphisec's prevention capabilities are not dependent on updates or patch availability; protection is in place even before a vulnerability has been discovered and a patch developed. With Morphisec, organizations can extend their patching cycles, reducing business disruption and risk at the same time.

Windows 7 PCI Compliance

Microsoft's ending of support for Windows 7 in January 2020 means that any endpoints and servers still running on Windows 7-based systems will not be updated or patched, and will make your entire POS network out of compliance with PCI DSS standards. Morphisec provides a mitigating technology that qualifies as a compensating control as defined by the PCI SSC. It also serves as a compensating control for any Windows 10-based deployments that are not fully patched.

Prevents Lateral Movement

Once an attacker has gained a foothold, they start to move laterally from machine to machine, traversing the network to find system resources and/or vulnerabilities they can exploit to escalate privileges, gain persistence and infect more devices. Morphisec stops lateral movement by making it impossible for the attacker to find the resources they need to move outside the initial entry point.

Zero Business Disruption

Morphisec uses a tiny 2 Mb agent with no runtime components and zero impact on endpoint performance. It operates invisibly to the end user, with no interruptions for updates or scans.

ABOUT MORPHISEC

Morphisec has revolutionized endpoint protection with its Moving Target Defense technology, which instantly and deterministically stops the most dangerous and evasive attacks while allowing companies to cut operational costs. With a true prevention-first approach to stopping zero-days, with no false positives, Morphisec eliminates the complexity and burden for organizations struggling to respond to cyberattacks.