Kaspersky® Embedded Systems Security

Point of Sale als Angriffsfläche: Bedrohungen für POS-Systeme

POS-Terminals (Point of Sales) sind spezialisierte Computersysteme, die zunehmend zum Ziel von Cyberangriffen werden. Oberflächlich betrachtet ähnelt ein elektronischer Kiosk oder Ticketautomat nicht einer Büroarbeitsstation oder einem Heimlaptop, aber diese POS-Terminals sind genauso anfällig für Cyberangriffe wie jedes andere intelligente prozessorbasierte Gerät. Und in gewisser Weise sind sie noch stärker bedroht.

Im Jahr 2014 ereignete sich ein Vorfall, von dem Millionen US-Bürger betroffen waren: Cyberkriminelle erhielten Zugang zu vertraulichen Daten von über 70 Millionen Kunden einer großen Einzelhandelskette und mehr als 40 Millionen Bankkarten. Die Untersuchungen ergaben, dass weder das Zahlungsverkehrssystem noch die Server des Unternehmens betroffen waren. Der Diebstahl wurde über infizierte Kassen und POS-Terminals durchgeführt. Von Cyberkriminellen auf diesen Geräten installierte Malware fing Zahlungsdaten ab, die unverschlüsselt im Arbeitsspeicher der Terminals abgelegt waren.

Der Vorfall zeigt, dass Cyberkriminelle nicht nur die Entwicklungstrends in der Zahlungsabwicklung durch Datenverarbeitungstechnologien und -geräte genau verfolgen, sondern auch fortlaufend spezialisierte Malware entwickeln, um diese neuen Entwicklungen auszunutzen und wertvolle Finanzdaten zu stehlen.

Man darf aber nicht davon ausgehen, dass dem Problem der Malware für POS-Endgeräte vor den aufsehenerregenden Hacking-Vorfällen dieser Einzelhandelsnetzwerke keine Beachtung geschenkt wurde. Doch obwohl POS-Malware bereits seit mindestens 2010 regelmäßig für Angriffe auf Unternehmen eingesetzt wurde, hatten POS-Cyberattacken bis zu diesem Zeitpunkt nicht die Aufmerksamkeit der allgemeinen Öffentlichkeit auf sich gezogen. Im Jahr 2010 wurde die Entdeckung von Trojan-Spy.Win32.POS (auch als CardStealer bekannt), der auf infizierten Workstations nach Zahlungskartendaten suchte und alle gefundenen Informationen an den Server der Cyberkriminellen schickte, weltweit in den Nachrichten verbreitet. Seitdem ist kein Jahr vergangen, ohne dass Anti-Malware-Experten neue Varianten von Malware entdeckt haben, die dazu dienen, Zahlungsdaten von POS-Terminals zu stehlen.

- 2010 • Trojan-Spy.Win32.POS (CardStealer)
- 2011 • Backdoor.Win32.Desty (Dexter)
- 2012 • Trojan-Spy.Win32.Vskim (vSkimmer)
- 2013 • BlackPOS (modified CardStealer)
- 2013 • Trojan.Win32.Fsysn (Chewbacca)
- 2014 • Backdoor.Win32.Backoff (Backoff)
- 2015 • LogPOS, Punkey, POSeydon, FindPOS

Heute besteht die Infektion von POS-Terminals aus weit mehr als nur punktgenauen Angriffen. Mit POS-Technologien haben Cyberkriminelle ein neues Sprungbrett für die Umsetzung von Bedrohungen gefunden, das einen besseren Zugang als je zuvor zum Geld anderer Menschen ermöglicht.

```
v2 = lstrlen("update=", v12);
if ( StrCmpNIA(v16, "update=", v2) )
{
  v3 = lstrlen("checkin:", v11);
  if ( StrCmpNIA(v16, "checkin:", v3) )
  {
    v4 = lstrlen("scanin:", v10);
    if ( StrCmpNIA(v16, "scanin:", v4) )
    {
      v5 = lstrlen("uninstall", v9);
      if ( StrCmpNIA(v16, "uninstall", v5) )
      {
        v6 = lstrlen("download=", v8);
        result = StrCmpNIA(v16, "download=", v6);
        if ( !result )
        {
          v19 = v16 + lstrlen("download=", v7);
          v16 = v19 + sub_151C80(&v15, v19, 59) + 1;
```

Abbildung 2: Einige der Befehle, die Dexter vom entsprechenden C&C-Server erhält

Allgemeine Betriebssysteme im Vergleich zu Spezial-Malware

Die bösartigen Aktivitäten von Cyberkriminellen werden dadurch erleichtert, dass es sich bei den POS-Geräten im Wesentlichen um gewöhnliche Computer handelt, die für „alltägliche" Aufgaben wie das Surfen im Internet und Lesen von E-Mails genutzt werden können (und dafür in kleinen Unternehmen oft auch verwendet werden). Diese Aktivitäten können Cyberkriminellen möglicherweise Fernzugriff auf die Geräte ermöglichen.

Ein Schadprogramm, das 2012 entdeckt wurde und den Namen Dexter erhielt, wurde beispielsweise entwickelt, um Bankkartendetails zu stehlen, indem POS-Terminals auf Windows-Basis angegriffen wurden. Der Malware-Code wurde in den Systemprozess „iexplore.exe" eingefügt, um den Inhalt des Hauptspeichers zu lesen und nach Zahlungsdaten zu suchen, mit denen eine gefälschte Plastikkarte erstellt werden konnte, d. h. Name des Karteninhabers, Gültigkeitsdatum und Kartennummer (einschließlich Ausstellercode), Kartenklasse und -typ, Kontonummer usw. Anschließend wurden die gesammelten Informationen auf einen Remote-Server hochgeladen, der von den Cyberkriminellen kontrolliert wurde.

Bevor Abwehrmaßnahmen ergriffen wurden, drang Dexter in Hunderte von POS-Systemen in bekannten Einzelhandels-, Hotel- und Restaurantketten sowie privaten Parkhäusern ein. Man kann mit ziemlicher Sicherheit davon ausgehen, dass auf den meisten betroffenen POS-Systemen Windows XP ausgeführt wurde.

Ein weiteres Beispiel ist der berüchtigte POS-Trojaner Backoff, der entwickelt wurde, um Zahlungskartendaten von Zahlungsterminals zu stehlen. Mit dieser Malware wurde wie bei Dexter der Hauptspeicher des POS-Terminals ausgelesen und nach Zahlungskartendaten gesucht. Darüber hinaus enthielten einige Versionen von Backoff eine Komponente zum Abfangen von Tastatureingaben (Keylogger), die vermutlich zum Einsatz kam, wenn der infizierte Computer kein POS-Terminal, sondern eine Workstation war (an der auslesbare Informationen per Tastatur eingegeben wurden).

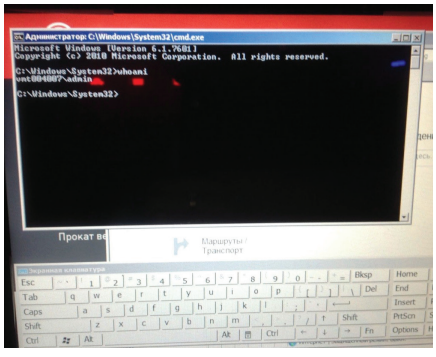


Abbildung 3: Beispiel für die Ausnutzung von Schwachstellen in Parkautomaten-Apps

POS-Systeme jenseits des Einzelhandels

POS-Geräte finden sich heute nicht nur in Handelsketten, Supermärkten und Hotels. Auf jeder Straße sieht man POS-Systeme zum Bezahlen der Parkgebühr oder benutzerfreundliche Kiosksysteme für das Laden eines mobilen Geräts. In Flughäfen und Bahnhöfen gibt es eine Vielzahl von Ticketautomaten und Informationskiosken, in Kinos stehen Terminals für die automatische Sitzplatzreservierung und den Ticketkauf bereit. In Wartezimmern und öffentlichen Einrichtungen gibt es elektronische Warteschlangenmanagement-Systeme. Heute verfügen sogar öffentliche Toiletten bisweilen über Zahlungsterminals.

Leider sind nicht alle diese Geräte ausreichend vor Cyberkriminalität geschützt. Im Sommer 2014 entdeckten die Experten von Kaspersky Lab Fehler in der Konfigurationssoftware von Fahrrad-Parkterminals, die den Zugriff auf den Speicher des Geräts und in weiterer Folge auf Benutzerdaten (einschließlich Zahlungsdaten) ermöglichten.

Eine Anwendung, die unter Windows ausgeführt wurde, ermöglichte es dem Nutzer der Fahrrad-Parkstation, sich zu registrieren und den Standort anderer Parkstationen sowie Bars, Cafés und anderer Objekte zu sehen. Diese Informationen werden über ein in das Gerät integriertes Google-Widget angezeigt. Der Benutzer kann die Vollbildanwendung zwar nicht minimieren oder das Fenster verlassen, die Anwendung weist jedoch einen Konfigurationsfehler auf, der den Zugriff auf das Gerät ermöglicht: Bei bestimmten Links – „Fehler melden", „Vertraulichkeit" und „Nutzungsbedingungen" – wird der Browser Internet Explorer gestartet, sobald der Benutzer darauf tippt.

Globale Kompetenz mit Technologien von Kaspersky Lab

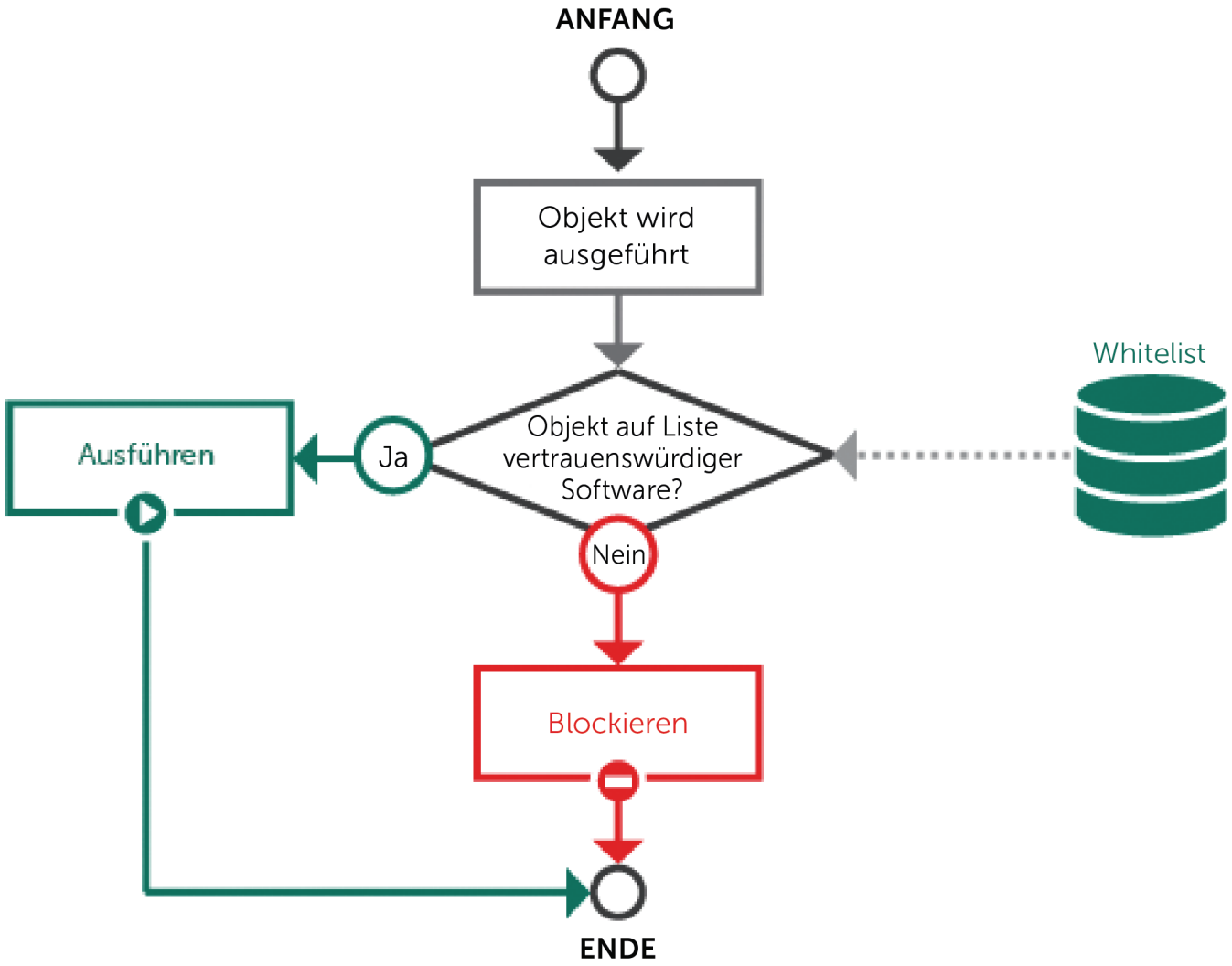
Die Ergebnisse unabhängiger Tests bestätigen regelmäßig die Wirksamkeit der Produkte von Kaspersky Lab. Im Jahr 2016 belegte das Unternehmen anhand der TOP 3-Metrik den ersten Platz unter den Entwicklern von Sicherheitslösungen. Den Ergebnissen von 78 verschiedenen Tests und Bewertungen angesehener Testorganisationen zufolge lagen die Lösungen von Kaspersky Lab in 90 % aller Ergebnisse unter den Top Drei und belegten 55 Mal den ersten Platz. Diese Tests belegen, dass Kaspersky Lab in der Branche führend ist, wenn es um die Qualität der Schutzmaßnahmen geht.

Konfigurationsfehler dieser Art können von Cyberkriminellen ausgenutzt werden. Beispielsweise können Angreifer das unverschlüsselt im Speicher abgelegte Administratorpasswort auslesen. Oder sie können auf den Datenspeicher der Fahrrad-Parkstation-App zugreifen. So können die persönlichen Daten der Benutzer aus Speicherauszügen extrahiert werden, einschließlich vollständiger Namen, E-Mail-Adressen und Telefonnummern – eine Datenbank mit verifizierten Adressen und Telefonnummern ist auf dem Schwarzmarkt der Cyberkriminalität immer besonders wertvoll. Ein Angreifer kann auch einen Keylogger installieren, der alle über die Tastatur eingegebenen Daten abfängt und an einen Remote-Server sendet, oder bei dem Angriff über zusätzlich implementierte weitere Dateneingabefelder sogar noch mehr Daten sammeln.

Point of Sale Security

Betriebssysteme von POS-Geräten sind Workstation-Betriebssystemen sehr ähnlich und anfällig für die gleichen Bedrohungen. Selbst wenn ein Terminal also nicht mit einem benutzerdefinierten Trojaner angegriffen wird, besteht immer das Risiko einer Infektion durch gewöhnliche Malware von Desktop-Betriebssystemen. Diese setzen das POS-Gerät genauso effektiv außer Betrieb und richten finanziellen Schaden an. Deshalb bietet die Sicherheitslösung von Kaspersky Lab für Embedded-Systeme Anti-Malware-Technologien zum Schutz vor allen Arten von Schadprogrammen, einschließlich solcher, die sich zwar nicht speziell an POS-Geräte richten, aber dennoch ein Betriebssystem befallen und ein Denial-of-Service-Ereignis auslösen können.

In der Welt der herkömmlichen Workstations und Server sind der Gedanke einer vertrauenswürdigen Umgebung https://securelist.com/computing-securely-the-trusted-environment-concept/57882/ und die dahinter stehende Whitelisting-Technologie längst weit verbreitet. Mit Default Deny und Whitelisting kann sichergestellt werden, dass nur die Software auf Firmencomputern ausgeführt werden darf, die für geschäftliche Aufgaben benötigt wird.



Über Kaspersky Lab

Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 1997 gegründet wurde. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen Einrichtungen sowie Privatanwendern weltweit. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexen und neu aufkommenden Cyberbedrohungen.

Mehr als 400 Millionen Nutzer und 270 000 Unternehmenskunden werden von den Technologien von Kaspersky Lab geschützt.

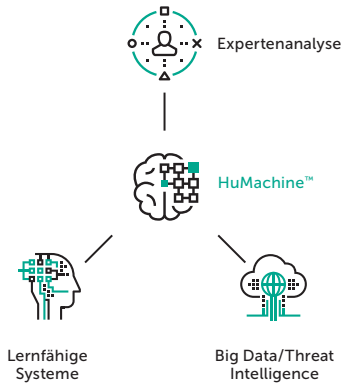
Weitere Informationen zu Kaspersky Lab finden Sie unter Kaspersky.de/enterprise-security

Die Experten von Kaspersky Lab haben Kaspersky Embedded Systems Security entwickelt, eine Sicherheitslösung für POS- und Geldautomatensysteme, die speziell für diesen Gerätetyp entwickelt wurde und Default-Deny-Technologien umfasst, um Embedded-Betriebssysteme vor den speziell auf sie zugeschnittenen Bedrohungen zu schützen. Wird die Sicherheitslösung auf einem Terminal installiert, folgt die Ausführung aller Anwendungen auf diesem Terminal diesem Szenario:

- Das Betriebssystem startet die Ausführung einer Anwendung, eines Skripts oder einer Bibliothek.
- Das Sicherheitssystem des Produkts überprüft anhand einer Whitelist vertrauenswürdiger Programme und Komponenten, ob die Anwendung, das Skript oder die Bibliothek vertrauenswürdig ist.
- Das Betriebssystem startet die Ausführung einer Anwendung, eines Skripts oder einer Bibliothek.

Default Deny-Technologien ermöglichen es, eine Betriebssystemumgebung für das POS-Terminal zu schaffen, die nur die Ausführung von Softwareanwendungen zulässt, die für das begrenzte Aufgabenspektrum des Terminals notwendig sind. Infolgedessen verläuft jeder Versuch von Cyberkriminellen, willkürlichen Code im laufenden Betriebssystem eines durch Default Deny-Technologien geschützten Terminals auszuführen, erfolglos.

Finanzunternehmen und Firmen, die POS-Terminals betreiben, sollten beim Schutz ihrer Geräte wachsamer sein und dabei nicht nur die Sicherheit von Hardwarekomponenten, sondern auch der Betriebssysteme und der gesamten vernetzten IT-Infrastruktur berücksichtigen. Um solch ein hohes Schutzniveau zu erreichen, können Unternehmen sowohl Sicherheitswerkzeuge, die in Unternehmensnetzwerken schon lange im Einsatz sind, als auch dedizierte Lösungen für Embedded-Systeme nutzen. Im unwahrscheinlichen Fall einer Sicherheitsverletzung ist es wichtig, schnell zu reagieren und mit Strafverfolgungsbehörden und Sicherheitsunternehmen zusammenarbeiten, um die Ursache des Problems zu ermitteln.



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise-security**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **www.kaspersky.de/blog/b2b**

#truecybersecurity
#HuMachine

www.kaspersky.de