גניבת פרטי אשראי מקופות דיגיטליות

מאת אלכסנדר גצין

הקדמה

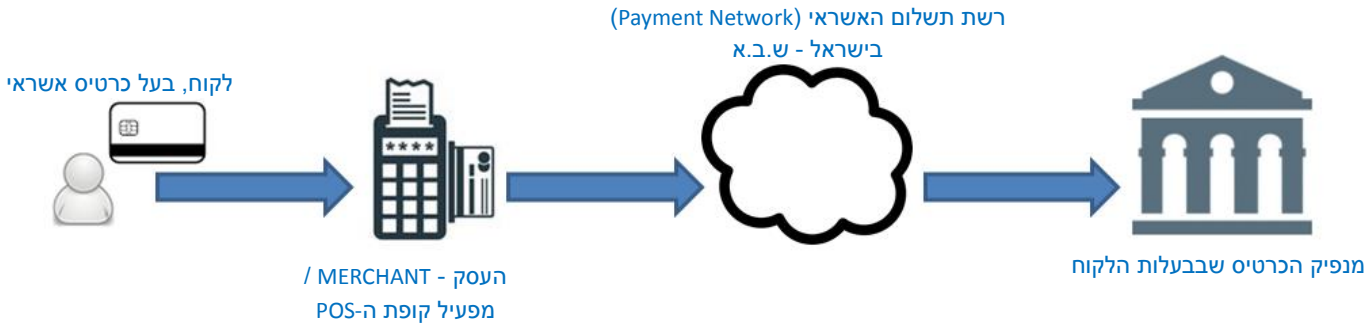
פריצות וגניבות פרטי כרטיסי אשראי בשנות 2013-2014 חשפו מעל מאה מיליון כרטיסי אשראי ונתון זה אינו כולל את פרטי הלקוח. חברות האשראי, בנקאות ומסחר סופגות הפסדים ותובעות את חברות הביטוח למימוש פוליסות. חברות אלה, נמצאות תחת רגולציה כבדה ומשקיעות משאבים רבים בפתרונות מידור הסיכונים וההפסדים (השקעת המשאבים גדלה ב-2016 לעומת אשתקד במרבית הארגונים בכ--20 40 אחוז) בהתאם.

בשנת 2016, תופעת הונאות אשראי וגניבת פרטי כרטיסים צפוייה להתרחב בהתבסס על ספקולציות, בפרט לאור המעבר לסליקה מבוססת כרטיס פיזי בסטנדרד EMV - מעבר לסליקת כרטיסים מבוססי צ'יפ ותעודה דיגיטלית, העברת אחריות ההפסדים ל-MERCHANT על הפסדים אם ה-MERCHANT לא תמך בטכנולוגיה. העולם עובר לכרטיסי אשראי עם צ'יפ = כרטיס אשראי חכם שימנע הונאות "פיזיות" (גניבת כרטיס אשראי), מעבר שינתב את פשע ההונאות בכרטיסי אשראי למרחב הדיגיטלי.

הגורמים שהוזכרו, התקפות מוצלחות על ה-POS-ים (Point Of Sale) והמעבר לסטנדרט שיקשה על הונאות כרטיס פיזי יגבירו את פעילות התוקפים בגניבת פרטי אשראי. מקור הסיכון הדומיננטי להפסדים הוא נמוך בשרשרת עיבוד האשראי - בחולייה החלשה כמובן, ה-POS וסביבת מחייתו הטבעית, המפעיל של הקופות החכמות (POS), בית העסק - ה-Merchant.

רקע - סליקה וקופות דיגיטליות

על מנת להבין איפה פרטי האשראי וקופות ה-POS נכנסים לתמונה, נבחן, במבט מעל את תהליך הסליקה הסטנדרטי כאשר לקוח מבצע רכישה בחנות (עסקה בנוכחות הרוכש, עם כרטיס אשראי):



ברגע שהלקוח מעביר את כרטיס האשראי שלו בעסק (MERCHANT), הסולק עמו העסק נמצא בהסכם מאמת את העסקה מול מנפיק הכרטיס, נבדקים נתונים כגון תוקף הכרטיס, מסגרת האשראי ועוד.
אימות העסקה חוזר ממנפיק הכרטיס ואל העסק, רשת התשלום, *שירותי בנקאות אוטומטיים* בישראל, מרכז את התקשורת בצורה מאובטחת בין הגורמים.

הערה: חשוב להכיר שישנם גורמים נוספים שהושמטו לטובת הפשטת התהליך: הסולק, מותגי האשראי ורשת התשלום הבינלאומית SWIFT משחקים תפקידי מפתח בתהליך הרכישה באמצעות כרטיס אשראי - הסליקה.

במקרה שלנו, נדבר על פרטי האשראי שקופות אוספות על מנת לבצע פעולות, אותם פרטים יקרי ערך אשר נתונים באיום מצד תוקפים:

- **PAN** - מספר כרטיס האשראי (Primary account number), הנפוצים נעים בין 8 ל-16 ספרות. על פיו ניתן לזהות את סוג הכרטיס, מנפיק הכרטיס, מותג הכרטיס ואת הכרטיס הספציפי (4-8 ספרות ימניות / אחרונות) **נשמר כמידע על הכרטיס**
- **TRACKS** (1,2) - מחזיקים מידע מזהה של כרטיס האשראי: ה-PAN, תאריך תפוגה ומידע טכני נוסף.
- **PIN** - הוא קוד בן הארבע ספרות אשר נדרש לאימות בעל הכרטיס בנוכחות הכרטיס, **לא נשמר כמידע על הכרטיס**.
- **CVV** - הוא קוד בן שלושה או הארבע ספרות אשר נדרש לאימות בעל הכרטיס בלא נוכחות הכרטיס, גם כן, **לא נשמר כמידע על הכרטיס**.

אותן קופות דיגיטליות (Point of Sale) קיימות במגוון צורות, יישומים, פלטפורמות ובהתאם, גם "סביבתם הטבעית" מגוונת - מחומרה ומ"ה ייעודיים ועד יישומי קופות WEB וענן.

בין ייצרניות וספקיות שירותי הקופה הגדולות בעולם מתבלטת ECR Software Corporation, מדורגת כמובילה בשוק גלובלי ומציעה שירותים ופתרונות מקצה לקצה, קופת ה-POS הקלאסית שלה (Catapult) מבוססת Windows ורצה על מגוון חומרה.

דוגמאות למשווקות ולמפתחות בישראל:

- ריטליקס (שרכשה על ידי NCR) לקופות מכירה ומשווקת קופות ושירותים תומכים, ביניהם גם בענן.
- Verifone שמציע שירותי טכנולוגיות סליקה מגוונות בנוסף לקופות מכירה, ביניהם שירותי סליקה וכרטיסי אשראי.

ה-POS-ים בעולם נבדלים על פי מערכות הפעלה, פלטפורמה, יכולות ועוד, להלן סוגן:

מבוססות Microsoft Windows:

קופות חכמות מבוססת מערכת הפעלה מבית Microsoft הן הנפוצות בעולם, מתחלקות לשני סוגים:

- אפליקטיבית
- הרחבה למערכת הפעלה Windows מארחת, לדוגמא, Posready 7 מבוססת על Windows 7, מותקנת ורצה על מערכות Windows

יתרונות: קלה להפצה והפעלה היות ומופצת על מערכות Windows עם דרישות חומרה גמישות.
חסרונות: פגיעות לשלל הפרצות שיתלוו למערכת ההפעלה ולחומרה המארחים, פגיעויות ברמת מערכת הפעלה WINDOWS וגם שירותים תומכים כגון MS11-100 ב-Net. (ניצול על ידי CVE-2011-3415 או הפניית משתמש מעמוד האימות לטובת גניבת Credentials לדוגמא).

מבוססות Embedded:

מערכת ההפעלה נבנתה והותאמה לחומרה יעודית ובמטרה יעודית - נקודת מכירה. לדוגמא, Windows Embedded for Point of Service, מבוססת Windows XP SP2 / Windows 8, 8.1.

יתרונות: ביצועים משופרים, התקנה והפעלה קלים יותר, רמת הקשחה Defulte-ית גבוהה (לא תתמוך בשירותים שאינם נדרשים לטובת ביצוע ייעודה).
חסרונות: עצם היות Embedded מקשה על תהליכים אופרטיביים כגון Patch Management, סובלת מפגיעויות מערכות Windows "קלאסיות".

קופות Proprietary:

קופות דיגיטליות של ייצרני חומרה / בתי תוכנה אשר מבוססות על מערכות הפעלה, חומרה ו/או אפליקציה בפיתוח פנימי.

לדוגמא, **Toshiba 4690 OS:** פיתוח שIBM שנמכר ב-2012 ל-Toshiba, בגרסא עדכנית של Version 6 (עדכנית ב-Release6). מערכת הפעלה שמיועדת לרוץ על מגוון רב של חומרות כולל קופות פיזיות, מספקת שירותי קופה, שירותי WEB תומכים, ניהול מערך קופות ועוד.

<u>יתרונות</u>: מערכת ההפעלה 'סגורה' (קוד המקור לא זמין ברשת, שימוש בתשלום בלבד) אשר נכתבה ע"י IBM לשירותי קופה ולא בוססה על Windows, משמעות הדבר - חסינה לרוב הפגיעויות הנפוצות שמתרכזות בקופות הנפוצות של Microsoft ומקשה על תהליכי האקספלויטציה ואיתור פרצות. נכון לכתיבת שורות אלו רק שתי פרצות מפורסמות לציבור ואף אחת מהן אינה בחומרה קריטית.
<u>חסרונות:</u> מערכת ההפעלה הייחודית תדרוש מיומנות מיוחדת לתחזוקה וידע שאינו נפוץ ליישום אבטחה. נכון, היא מותקפת פחות מ-Windows אך אין זה אומר שהיא חסינה. ארגון אשר מקווה מטרה נאה מספיק לתוקף יכול למצוא עצמו מתקשה להתמודד תוקף מאובזר ב-0day, אם לא הכין עצמו בהתאמה (Incident Response ,Disaster Recovery).

מבוססות Open Source:

קופות קוד פתוח. קוד האפליקציה זמין ברשת לקהילה, נסקר לעומקיו בפומבי, בנוי לקסטומיזציה (התאמה) לצורכי המפעיל. כל אחד יכול להוריד ולהפעיל אותה, בדרך כלל - בקלות. וכן, חינם.

לדוגמא, **LemonPOS**: זמינה בגרסה ייצורית מ-2009 (BETA מ-2007), קופה דיגיטלית שניתן גם היום להוריד מאתר קהילת המפתחים הישן שלה וב-Sourceforge. מיועדת להרצה על Linux, בסיס נתונים MySQL, ממשק משתמש מבוסס Qt4. קוד האפליקציה זמין - מכך ההכרח הוא יישום אבטחה By Design (במקום להסתמך על חשאיות הקוד) ולא נמצאות בו חולשות קריטיות פרט לחבילות פרטניות שדורשות עדכון.

<u>יתרונות</u>: כן, חינם. פעמיים כי טוב. נבנה להיות קלה להפעלה, התקנה, פיתוח והתאמה לכל צורך. נסקרת ומדוברת, מה שחשוב כשמדובר במוצר Open Source. מספקת שירותים בסיסיים נדרשים כגון ניהול מלאי והדפסה.
<u>חסרונות</u>: לא מאטים לצד יתרונות משמעותיים - אין תמיכה. מה שמציג סיכון למפעיל שאין לזלזל בו.

אין עדכונים, המפעיל נדרש לפתח את הקופה בכדי לעמוד באיומים של היום (לדוגמא לעדכן חבילות TLS עדכניות על ההתקנה הבסיסית). קוד האפליקציה זמין - ניתן לפתח ולתכנן תקיפה בקלות במידה ונמצאה פגיעות / חולשת אבטחה.

Cloud POS:

שירותים Software as a Service או תצורות היברידיות אשר מנגישים ללקוח מגוון יכולות וכלים שמתאפיינים ברמת אבטחה גבוהה ותאימות עם סטנדרטים אך גם סיכונים מובנים יחודיים. אפליקציית הקופה נגישה ללקוח בממשק WEB-י ומאפשרת סליקה ללא נוכחות כרטיס (CVV + PAN) או חיבור מאובטח אל יחידה פיזית בצד הלקוח שסולקת כרטיסים. ספקים רבים, גדולים וקטנים כגון **Microsoft, Amazon, Verifon**, **WebPOS** ועוד מציעים שירותי סליקה בענן.

<u>יתרונות</u>: עיבוד האשראי מינימאלי בצד 'מפעיל' הקופה מה שמקטין סיכונים רבים ומקל על תאימות לתקינה, חוק ורגולטורים. שירותי ענן מסוגלים לספק ביצועים וזמינות מאוד טובים. אחריות לאבטחה על תשתית עיבוד האשראי עוברת לספק השירות, לצד אופרציות אבטחה (כגון ניהול עדכונים / פגיעויות ועוד).

<u>חסרונות</u>: הנוחות ורמת האבטחה המובטחת מצד ספק השירות מתעתעים בצרכן: אומנים סיכונים רבים ממועברים - אחרים, יחודיים נכנסים לתמונה. שירות הסליקה הוא אופרציה קריטית לרוב העסקים וסליקה מול ענן מפתחת תלות מלאה בחיבור האינטרנט. התוקפים אינם עיוורים למגמות בעולם, בפרט בעולם הסליקה - פורסמו סקירות של תקיפות ממוקדות על שירותי ענן (לדוגמא Account Hijacking) ו-Malwares ממוקדים (POSCloud שמנצל פרצות בדפדפן מפעיל הקופה / מנהל השירות לגניבת מידע אשראי). איומי ענן מורכבים נכנסים לתמונה - דיירי שירות מקבילים, נגישות לשירות (ומידע האשראי שאתה מעבד) מרשת האינטרנט, וספק השירות בעצמו מציגים סיכונים שיש לנהל.

למרות המגוון, רוב הקופות הדיגיטליות בשטח הן גרסאות של מערכת הפעלה (ניחשתם) Windows. קופות דיגיטליות מבוססות Windows הן הנפוצות בעולם ומהוות כיעד ההתקפה הנפוץ מקופות ה-POS.

איומים, ווקטורי תקיפה

מה הוא ווקטור תקיפה, מדוע חשוב להכיר אותם ואיך להפיק תועלת ישימה מסקירתם?

ווקטור תקיפה הוא אפיק בו לתוקף יש ממשק עם הארגון או יכולת להשפיע על מערכות המידע שלו. בין אם ע"י קלט צד משתמש באתר WEB, ניצול תהליכי עבודה כגון הורדת והתקנת עדכונים, תקיפה פיזית כגון ניסיון עקיפת מנגנוני בקרת גישה פיזיים ע"י Tailgating (להיכנס אחרי עובד מאושר כאשר זה פתח דלת ע"י הזדהות). מדובר במושג כללי (יותר מ-Attack Surface לדוגמא, שידבר על שדות קלט ועוד), חשוב מאוד שארגון יכיר איך ניתן לתקוף אותו, יישם בקרות הדוקות ומרובות שכבה באפיקים אלו.
מתוך הערכת ווקטור תקיפה לארגון מסיקים תמונה כוללת של **האיומים** שהארגון חשוף אליהם בתקיפת סייבר (פעילות זדונית אשר תפגע בארגון למטרה כזאת או אחרת).

איומים

ארגון אשר מפעיל קופות חכמות הוא ארגון שמשדר פרטי אשראי, סביר מאוד להניח שבין אם הוא מכיר בכך או לא - הוא גם מאכסן ומעבד אותם. אותו ארגון, מחויב לכל הפחות לשמירה על פרטיות מידע אישי על פי חוק ברוב המדינות בעולם, לשמירה קפדנית יותר של פרטי אשראי ע"פ הנחיות רגולטורים. בין מחויב הארגון בישירות או לא, עליו לנהל סיכונים.

בכדי להבטיח רמת אבטחה לקהל לקוחותיה, עמידות הארגון מבני הפסדים ולהבטיח לעצמם קלף מכריע בבתי משפט ההנהלה הבכירה בארגון תנחה ליישם ניהול סיכונים, פן חשוב מאוד הוא סיכוני א"מ וסייבר.
ע"י מתודולוגיית OWASP ואחרות, מושגי הערכת סיכון למערכות מידע תחושב כמותיץ בצורה הבאה:

Risk = Threat * Vulnerability

איום הוא אירוע בעל סבירות לגרום נזק, נפרט את האיומים הרלוונטיים לארגונים הפעילים קופות חכמות:

קופת ה-PC אליה ה-POS מחובר:

- התקפות APT ו-Phishing על עובדי/רשת הארגון לגניבת מידע אשראי ו-PII
- ניצול פגיעויות והפצת Malware ייעודיים לגניבת מידע אשראי

בסופו של דבר, במקרים רבים ה-POS יכול לחשב כ"עוד עמדת קצה" ברשת הארגון והיא חשופה לתקיפות ברשת. במקרים אחרים, תקיפת עמדת הקצה המחוברת ל-POS גם היא עלולה לסכן ברמה גבוהה את הקופה עצמה.

במקרים בהם העמדה מריצה תוכנות יעודיות שנועדו לנהל את החנות / מידע אודות לקוחות (כגון חברי מועדון וכו').

[http://www.2mcctv.com/blog/wp-content/uploads/2012/06/pos-integration.jpg]

ה-POS עצמו:

- הפעלת RAM Scraping על הזיכרון הנדיף של מכשיר ה-POS עצמו בטרם מידע האשראי מוצפן – טכניקה המאפשרת, בהינתן יכולת לרוץ על אותו ה-CPU שעליו רצה תוכנת ה-POS עצמה (נפוץ בעיקר במקרים בהם עמדת ה-POS מבוססת Winodows) לבצע Dump לזיכרון של התהליך ובכך להשיג את הפרטים המוצפנים בעודם מפוענחות בזיכון המכשיר.

דוגמאות ל-Malware יעודיים ל-POS בעלי יכולות כאלה הם: JackPOS, BlackPOS, Backoff ו-Soraya, ניתן לקרוא עליהם עוד בדו"חות של חברת TrendMicro ו-Symantec בקישורים הבאים:

- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf
- קורא מגנטי מושתל "Card Skimmer" על גוף קורא הכרטיס (פיזית, מחוץ ל-Scope)

[https://www.wirecard.com/products/payment/pos-terminals]

מדובר במתקפה ישנה יחסית אשר צוברת תאוצה ואנו שומעים עליה יותר ויותר עם הזמן, הדרישה מצד התוקפים הינה - גישה פיזית. ניתן לקרוא על הנושא בפוסט מעולה של Brian Kerbs בקישור הבא:
http://krebsonsecurity.com/category/all-about-skimmers/

תווך התקשורת:

- האזנה לכבל שבין קורא הכרטיס לקופה (פיזית, מחוץ ל-Scope)
- תקיפות הרכיבים או תיווך התקשורת כאשר מדובר ב-POS שאינו מקומי (כגון Cloud\WebPOS), לעוד דוגמאת:

http://www.scmagazine.com/researchers-spot-flaws-that-could-allow-mitm-attacks-on-german-pos-systems/article/462538/

האיומים שנסקרו הינם בסיס ייסודי (Baseline) לסקירת איומים עבור ארגון המפעיל קופות POS, זה הוא בסיס טוב להתחיל ממנו את הערכת הסיכונים הפנימית או לגבש הנחייה ליישום בקרות. חשוב לא לשכוח שאין אפשרות לכסות את כלל התרחישים במאמר וכל מקרה דורש התאמה (Tailoring) וסקירת מקיפה ייעודית.

מקורות חיצוניים:

שותפים, ספקים ושירותים מהווים מקור לסיכון זליגת מידע האשראי, עם זאת גם במקרים כגון Target בהם התוקף השיג גישה ל-POS-ים של הרשת דרך ספק, ווקטור התקיפה היה תקיפת ה-POS עצמו.

ניתוח תקריות

להלן טבלה הסוקרת מקרי תקיפת POS שונים, הטבלה מציגה את כלי התקיפה שזוהה, את וקטור התקיפה, את העסק הנתקף ואת השנה בה התקיפה התקיימה.

Characteristics	Theft & exfiltration Method	Breach	Victim / date	Malware
BlackPOS ver2 code significantly different than BlackPOS1 except for exfiltration. Also dubbed FrameworkPOS	Ram Scraper, data saved to fake obfuscated dll file, to compromised external server, to ftp	Third party"s network	Target , 2013	**BlackPOS**
Low detection rates due to File injector, evidence cleanup & low profile attacks	Ram Scrapper to Encrypted(later versions) file, to hardcoded external ftp server	TeamViewer weak configured passwords, other misconfigurations and known CVE	Retailers, 2011-today	**Cherry-picker**
Similarity to target breach,	Ram Scrapper to file, to external server	stolen Third party credentials, unpatched WIN systems, outdated Windows XP Embedded SP3, pos OS	HomeDepot, 2015	**(?)** Some speculate BlackPos. Though unlikely
Malware framework, highly modular, emphasis on obfuscation and persistence, modular, professionally developed framework, difficult to detect because all hashes are unique to the victim system	Ram Scraper, APT hacking - & data theft & exfiltration varies	Exploitation of various vulnerabilities, leverage by dropper malware, Every module is a rootkit	Us Retailers ת2013-today	**ModPOS**
Breach was not appropriately handled by hired Incident response vendor. Reaccured. Assumed persistence & obfuscation mechanisms.	Assumed ram scraper, theft through compromised VPN	Compromised Virtual Private Network (VPN)	Affinity Casino, 2013	undisclosed
Pos & credit info malware is on the rise		PoS update method, breach of body of trust(Certificate chain), Bootkits : Spy.Banker	Mostly Retailers	**MORE**

המלצות

1. ליישם את המסקנות הפנימיות על בסיס ממצאי המחקר שמרוכז בטבלה הנ"ל.
2. בידול עמדות ה-POS מהרשת הארגונית וחיבורה אך ורק בנקודות בהן ישנו הצורך ובעזרת קישורים מאובטחים. במידה ואפשר - ניתוק העמדה לחלוטין מהרשת הארגונית ושימוש ברשת VPN יעודי.
3. להעשיר ולמקד את הערכת הסיכונים על בסיס עמודות ה-Breach ו-Theft\Exfiltration.
4. שימוש בתווך תקשורת מוצפן בין עמדות ה-POS לבין הרשת החיצונית, שימוש בהצפנה בין תוכנת ה-POS לבין החומרה.
5. להעשיר ולמקד את המתודולוגיה הארגונית להתמודדות עם אירועי סייבר וסיכוני סייבר הן ברמת מדיניות והן ברמת נהלי תגובה, בפרט על סמך עמודות Breach ו-Theft & exfiltration Method.
6. התקנת תוכנות Antivirus יעודיות / בעלות מודולים יעודיים לעמדות POS.
7. התקנת רכיבי IPS/IDS ברשת ה-POS לטובת איתור אנומליות בתקשורת.
8. ביסוס תרחישי תרגול סייבר שנתיים / בדיקות חוסן על סמך התרחישים שמתועדים במחקר.

לסיכום

מחזיקי פרטי (כרטיסי) האשראי נתונים תחת סיכונים מורכבים הנובעים כתוצאה מהצרכים העסקיים של החברות, הדואגות לשפר את זמינות וניידות פתרונות האשראי ללקוחות מחד ומאידך, זמינות, היכולת והמוטיבציה (רווחיות) של תוקפים להשיגם. את רוב ההתקפות המוצלחות והרועמות אנו צופים בסביבת ה-Merchants - הסוחרים, האחריות של חברות האשראי לנזקים אינה מכסה אותם כאשר מדובר במידע אשראי שאבד מסביבתם, במיוחד היות ואין הם עמדו באחריותם לאבטחה נאותה. אין זה אומר שחברות האשראי אינן חסינות כלל, אך החוליה החלשה במקרה של פרטי האשראי היא סוחרים, בפרט וסביב נקודת המכירה, הקופה הדיגיטלית, ה-POS.

על מחבר המאמר

אלכסנדר גצין, מנהל פרויקטי אבטחת מידע מטעם חברת EXTREME. מומחה אבטחת מידע מרקע טכני, התחיל את דרכו בממר"ם, מאז מילא תפקידי הדרכה, Analyst אבטחה, אינטגרציה, ניהול פרויקטים ותפקידים אחרים בתחום אבטחת מידע ותקשורת. לאלכס הסמכות טכניות בתחומי התקשורת (CCNA), אבטחת מידע (צוות התערבות, ניתוח ו-SIEM), מערכות אבטחה וטכנולוגיות (CCSE, CA,SYM SIEM ועוד) ואבטחת ענן (CCSA).

מקורות לקריאה נוספת

- https://www.sans.org/reading-room/whitepapers/analyst/understanding-preventing-threats-point-sale-systems-36332
- http://securityaffairs.co/wordpress/41928/malware/cherry-picker-pos-malware.html
- http://securityaffairs.co/wordpress/41933/cyber-crime/central-shop-black-market.html
- http://www.ehackingnews.com/2015/11/researchers-find-new-pos-malwares.html
- http://www.darkreading.com/vulnerabilities—threats/cherry-picker-pos-malware-has-remained-hidden-for-four-years/d/d-id/1323128
- http://krebsonsecurity.com/tag/blackpos/
- http://www.darkreading.com/home-depot-breach-may-not-be-related-to-blackpos-target/d/d-id/1315636
- http://www.isightpartners.com/2015/11/modpos/
- http://www.digitalcheck.com/business-and-bank-resources/2014-03-07-23-06-29/pos-encryption-understanding-the-basics
- https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367
- http://www.scmagazine.com/researchers-spot-flaws-that-could-allow-mitm-attacks-on-german-pos-systems/article/462538/