



Stuxnet

אמיר טטלבאום

מי אני

▶ מייסד חברת סייבריה

▶ חוקר חולשות Malware מגמות וגופים שונים בעולם הסייבר

▶ מרצה בקורסי Cyber Warfare Defence | Hacking Defined Expert



סטאקסנט במספרים

- ▶ ~131072 מחשבים נגועים
- ▶ ~65536 מחשבים באיראן
- ▶ ~32768 מחשבים שאיראן אישרה שנדבקו
- ▶ ~1024 צנטריפוגות הרוסות
- ▶ 8 שיטות התפשטות שונות
- ▶ 4 פגיעויות לא מוכרות (0-Day)
- ▶ 2 חתימות דיגיטליות גנובות



2 ב-10, רק היום !



▶ שוק הפגיעויות פורח, יותר ויותר חוקרים מתפרנסים ממנו כמקור הכנסה ראשון

 Sticky: private office exploit { .doc }
Started by bad-sector, 05-06-2011 02:48 [1](#) [2](#) [3](#) ... [12](#)

Replies: 110
Views: 8,637

bad-sector
3 Days Ago 22:35 

 Sticky: EXPLOITS
Started by darkcoderz, 22-11-2010 01:49 [1](#) [2](#) [3](#) ... [19](#)

★★★★★
Replies: 186
Views: 22,592

keztex
8 Hours Ago 23:22 

▶ הפגיעויות בסטאקסנט שוות בשוק מעל \$500000

darkcoderz
Senior Member

EXPLOITS

MS OFFICE and PDF EXPLOITS
i have various exploits to offer like -
office 2007 exploits doc, ppt ,xls
pdf exploits
exploits for 2003 also i have but since some of them leaked on forum already
customized exploits for office and pdf are also there
all exploits are very private and FUD
for sample ,creator and source code pm me.
msn fed.degna@hotmail.com
skype darkblackcoders1

 [paradoxis](#) and [Ted Bundy](#) like this.

כרוניקה של סטאקסנט



מי אתה סטאקסנט ?



▶ פצצת סייבר

▶ אוטונומי לחלוטין

- מכיל את כל תהליך התקיפה ב-Payload בודד
- מתקשר עם 2 שרתי C&C בלבד
- מתקשר בסביבת LAN בעזרת P2P

▶ גנרי לחלוטין

- לא איראן ולא שום יעד מוגדר אחר מופיעים בקוד
- השפעה על רכיבי PLC שהם ממירי תדר
- אין קשר לגרעין ! בטח ובטח לא לצנטריפוגות

▶ חמקמק, אך במידה

- שימוש בחתימות דיגיטליות גנובות ע"מ להתחמק מאנטי-וירוסים
- שימוש ב-Rootkit להסתרה של הקבצים שלו
- לעומת זאת – הקוד אינו מוצפן, ללא יכולות Anti-debugging

למה לקח כל כך הרבה זמן לתפוס את סטאקסנט?



▶ לא עושה נזק למחשב

▶ לא מוציא חומר מהארגון הנתקף

▶ שימוש בחתימות דיגיטליות גנובות

▶ שימוש בחולשות לא מוכרות

▶ מנגנוני בלימה

◦ תקשורת עם שרתי C&C שמאפשרת קבלת פקודת התאבדות

◦ הגבלת הדבקה באמצעות DOK למקסימום 3 דילוגים

◦ תאריך Deadline – 24/06/2012

▶ החדרה באזור גיאוגרפי ספציפי

הטכנולוגיה מאחורי סטאקסנט

- ▶ סטאקסנט מציגה מספר חסר תקדים של 4 חולשות 0-Day
 - MS10-046 – חולשה בקבצי LNK, משמשת להתפשטות בDOK
 - MS10-061 – חולשה בPrint Spooler, משמשת להתפשטות ברשת
 - MS10-073 – חולשה בKeyboard Layout, משמשת לPE
 - MS10-092 – חולשה בTask Scheduler, משמשת לPE
- ▶ 2 חתימות דיגיטליות גנובות
 - Realtek Semiconductor Corps
 - JMicon Technology Corps

MS10-046

- ▶ באג דיזיין בקבצי LNK
- ▶ קבצי LNK יכולים להצביע לקבצי CPL (שהם DLLים)
- ▶ הקוד הפגיע מנסה לטעון אייקונים מתוך קבצי הCPL
- ▶ טעינת קבצי הCPL לטובת חיפוש האייקון מריצה את הCPL
- ▶ קורה בכל פעם שמסתכלים על תיקיה

MS10-061

▶ חולשה ב- Print Spooler Service

▶ מאפשרת "הדפסה" מרחוק של קובץ

- הקובץ נשמר תחת תיקיית %SystemRoot%\System32 לפי בחירתנו
- תוכן הקובץ שנשמר בשליטתנו
- שם הקובץ שנשמר בשליטתנו

▶ הדפסת קבצי MOF לתיקיית %SystemRoot%\System32\wbem\mof

- קבצים בתיקיה זו רצים באופן אוטומטי

MS10-073

- ▶ חולשה במנגנון Keyboard Layout של חלונות
- ▶ העלאת הרשאות ממשתמש רגיל לKernel
- ▶ מבוססת על טעות בבדיקה של מערך מצביעים לפונקציות

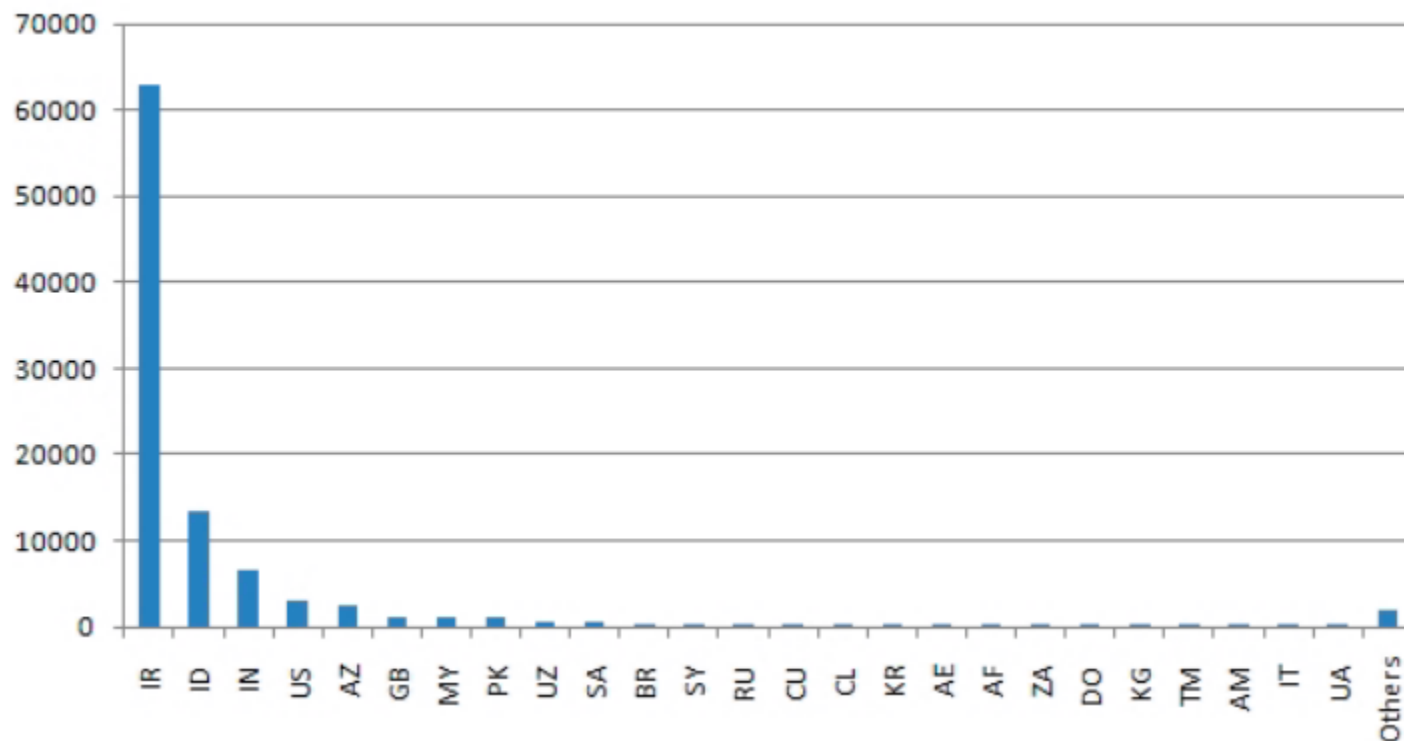
cf12fa38	cf933423	win32k!KbdNlsFuncTypeDummy	[index 0]
cf12fa3c	cf93342e	win32k!KbdNlsFuncTypeNormal	[index 1]
cf12fa40	cf933474	win32k!KbdNlsFuncTypeAlt	[index 2]
cf12fa44	ff496867		[index 3]
cf12fa48	ff466564		[index 4]
cf12fa4c	60636261	<- user space address	[index 5]
cf12fa50	0000006e		.

MS10-092

- ▶ חולשה בTask Scheduler של חלונות
- ▶ כל משתמש יכול ליצור משימה אשר תתבצע בעתיד (בהרשאות שלו)
- ▶ משימות נשמרות בתיקיית `C:\windows\system32\tasks`
- ▶ כל קובץ משימה מכיל את ההרשאות שאיתן תתבצע המשימה
- ▶ מה מונע מאיתנו לשנות את ההרשאות הללו לאחר יצירת המשימה?
 - קיים מנגנון חתימה דיגיטלית על הקבצים ☹️
 - מנגנון החתימה הדיגיטלית הוא CRC32 😊

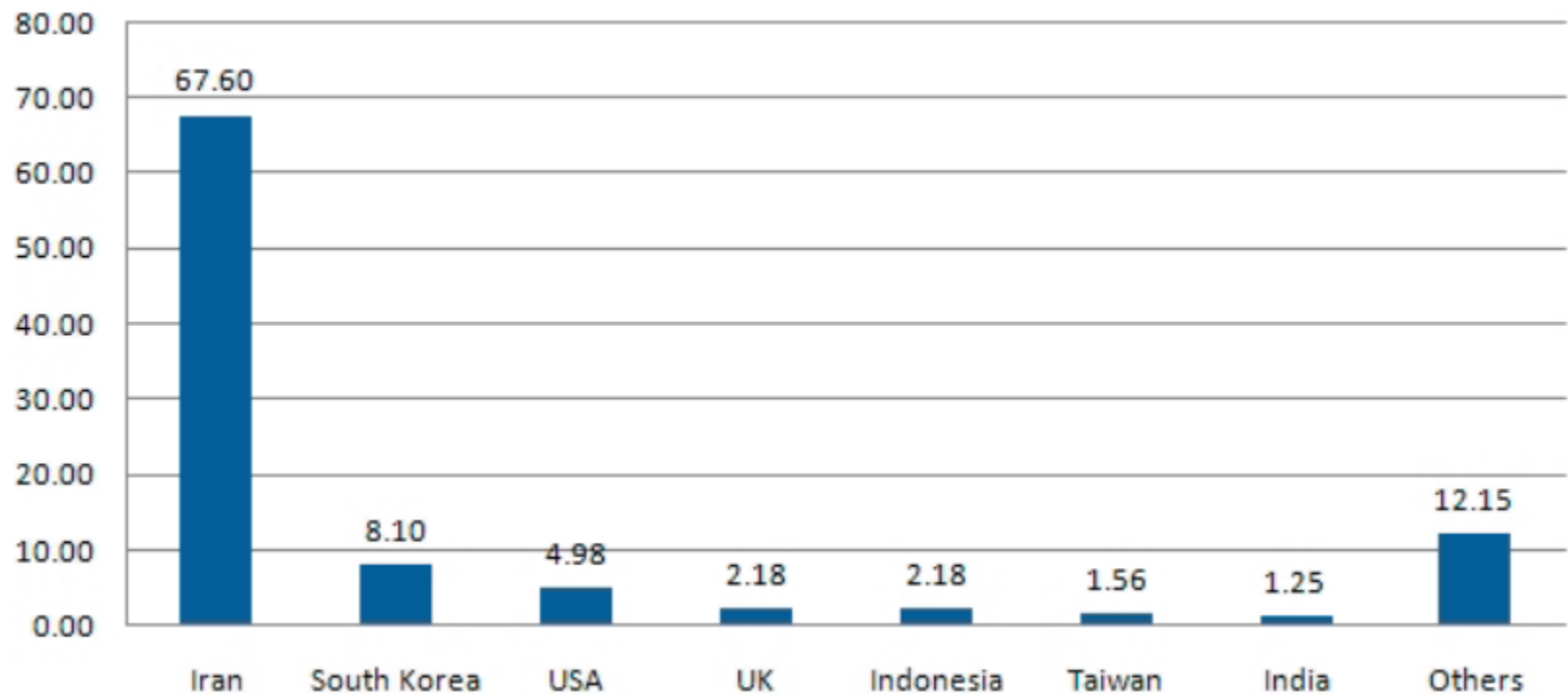
היעד של סטאקסנט

Infected Hosts

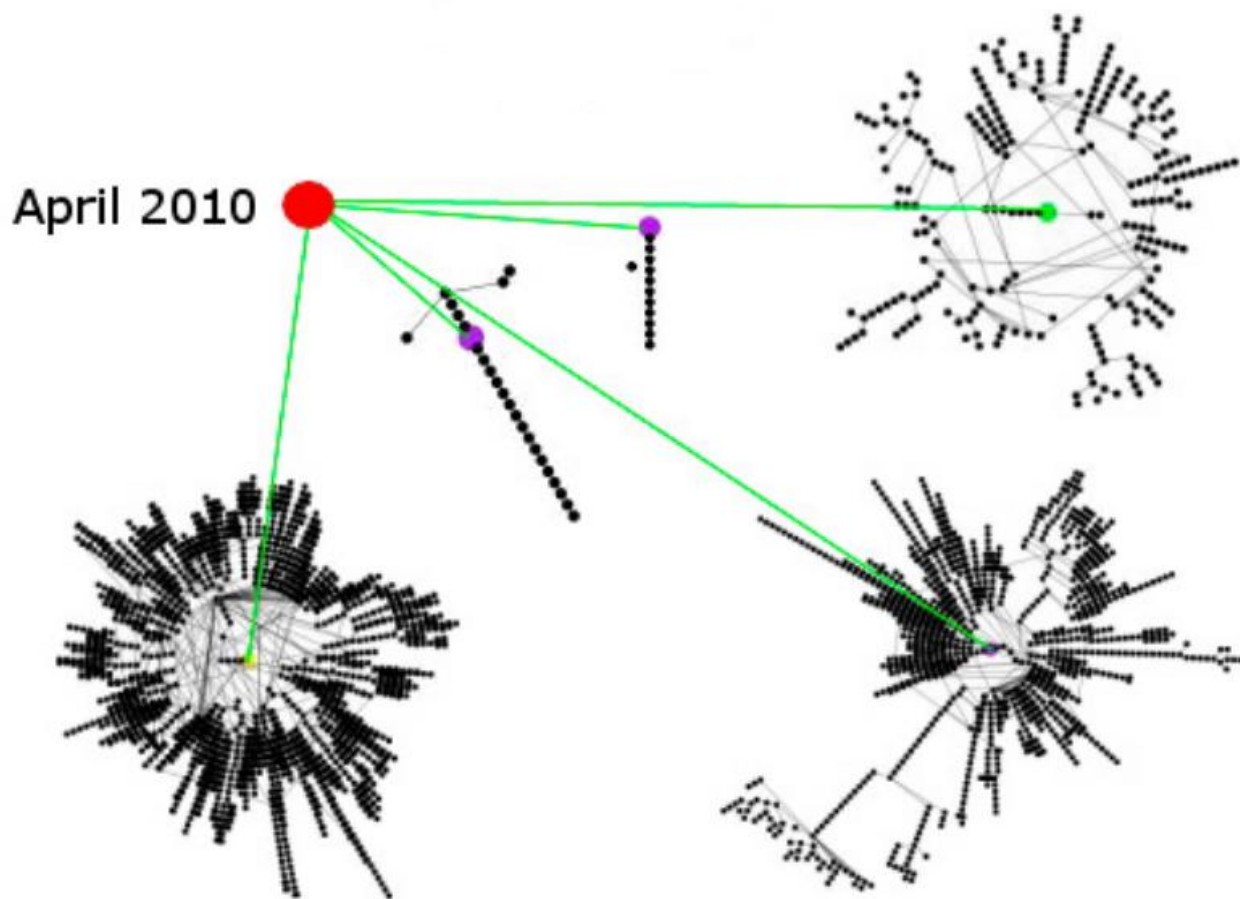


היעד של סטאקסנט

Percentage of Stuxnet infected Hosts with Siemens Software installed



היעד של סטאקסנט



היעד של סטאקסנט

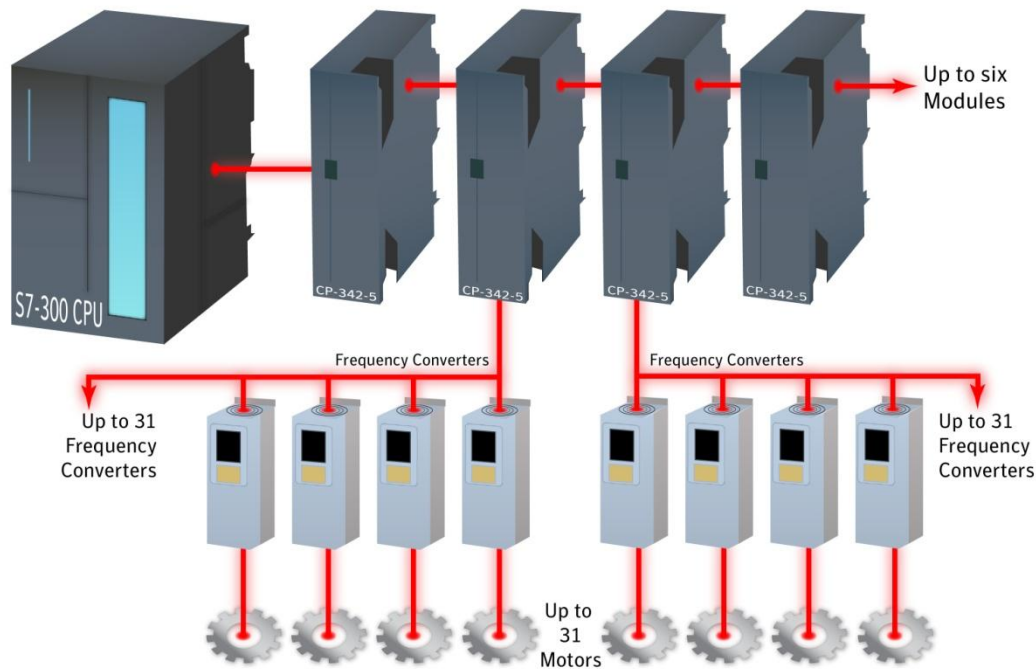
‣ בקרי SCADA של חברת סימנס

‣ לא סתם בקרי SCADA:

6ES7-417 ○

6ES7-315-2 ○

CP 342-5 ○



היעד של סטאקסנט

- ▶ תדר עבודה תקין של קסקדה נע בין 807Hz ל 1210Hz
- ▶ סטאקסנט משנה את תדר העבודה ל 1410Hz לפרק זמן מסוים, ואז מוריד בבת אחת את תדר העבודה ל 2Hz
- ▶ שינויים קיצוניים אלה, פוגמים גם בתפוקה וגם בקסקדה עצמה, עד כדי שבירת הציר

סטאקסנט כשינוי פרדימה בעולם הסייבר

▶ Cyberspace is real – השפעה גם בעולם המוחשי

▶ פצצות סייבר כבר לא Science Fiction

▶ עולם הסייבר הפך ל"חזית החמישית" של המלחמה

▶ הבנה שגם בעולם הסייבר קיים Collateral Damage
◦ סימנס מדווחת על לפחות 19 לקוחות אחרים אשר נדבקו



סטאקסנט כשינוי פרדימה בעולם הסייבר

▶ לקט הרצאות "חמות" מ BlackHat האחרון

Exploiting Siemens Simatic S7 PLCs ◦

Vulnerabilities in Wireless Water Meter Networks ◦

Battery Firmware Hacking ◦

Hacking Medical Devices for Fun and Insulin: ◦
Breaking the Human SCADA System

Open Source Cyber Weapon

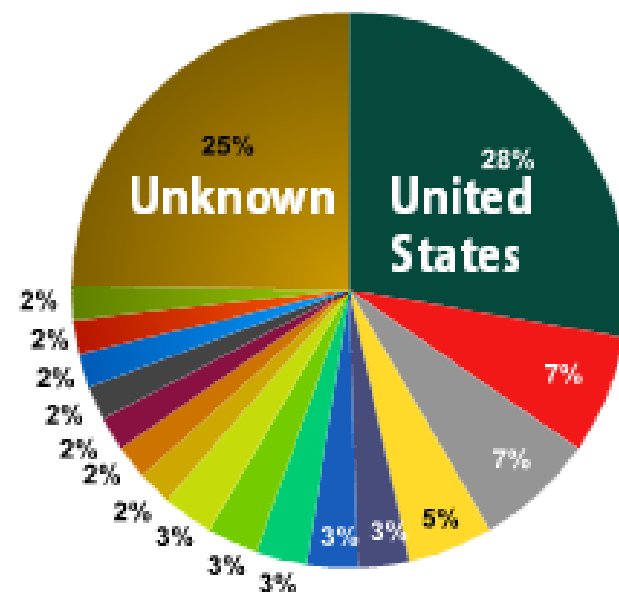
TDL4 Starts Using 0-Day Vulnerability!

0.4

In early December, Kaspersky Lab experts detected samples of the malicious program TDL4 (a new modification of TDSS) which uses a 0-day vulnerability for privilege escalation under Windows 7/2008 x86/x64 (Windows Task Scheduler Privilege Escalation, [CVE: 2010-3888](#)). The use of this vulnerability was originally detected when analyzing Stuxnet.

CyberCrimen נעזר בסטאקסנט

ותוקף בחזרה בארה"ב



Open Source Cyber Weapon

► הקוד של סטאקסנט מסתובב באינטרנט

The Stuxnet Source Code Available Online!

JULY 4, 2011 23:25 PM · 0 COMMENTS by BLACK on JULY 4, 2011

24
tweets

in MISCELLANEOUS, SOURCE CODE

retweet

We are publishing Stuxnet [source code](#) as it is available online. For educational or R&D purpose only! Yes, this is decompiled using the Hex-Rays decompiler.

Stuxnet is a [Microsoft Windows](#) computer worm discovered in July 2010 that targets industrial software and equipment. While it is not the first time that crackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) [rootkit](#).

Stuxnet is designed to programmatically alter Programmable Logic Controllers (PLCs) used in those facilities. In an ICS environment, the PLCs automate industrial type tasks such as regulating flow rate to maintain pressure and temperature controls.

Stuxnet targeted five Iranian organizations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran; Symantec noted in August 2010 that 60% of the infected computers worldwide were in Iran. Siemens stated on November 29 that the worm has not caused any damage to its customers, but the Iran nuclear program, which uses embargoed Siemens equipment procured clandestinely, has been damaged by Stuxnet

Download [Stuxnet source code](#) [Here](#)

► רק מחכה לשימוש חוזר

Welcome

This Blog is for Malware Researching, Reverse Engineering and System Programming

Reversing Stuxnet's Rootkit (MRxNet) Into C++

Posted by AmrThabet on 6:53 PM

Hello Again

```
633 if (Length < 1) { //mean couldn't be divided by 2 (That's will be strange because it's
634 EntryPtr = UserBuffer;
635 UserBuffer += NextEntryOffset;
636 (ULONG)UserBuffer != 0xD1; //over byte ptr [ebp+UserBuffer+3], 1
637 PrevOffset = NextEntryOffset;
638 continue;
639 }
640 Length -= FileNameOffset; //I don't know why
641 Length /= 2; //number of characters
642 if (((FileSize.u.HighPart != 0) && (FileSize.u.LowPart != 0)) || (FileSize.u.HighPart == 0
643 if (FileCheck(L"\\.\\" + FileName, Length - 1, 0) != 0) {
644 xmove(UserBuffer, UserBuffer + NextEntryOffset, PrevOffset - NextEntryOffset);
645 PrevOffset = NextEntryOffset;
646 continue;
647 }
648 }
649 if (FileCheck(FileName, Length, FileSize.u.LowPart, FileSize.u.HighPart) == 0) {
650 EntryPtr = UserBuffer;
651 UserBuffer += NextEntryOffset;
652 (ULONG)UserBuffer != 0xD1; //over byte ptr [ebp+UserBuffer+3], 1
653 } else {
654 if (NextEntryOffset != 0) {
655 xmove(UserBuffer, UserBuffer + NextEntryOffset, PrevOffset - NextEntryOffset);
656 } else {
657 if (EntryPtr != 0) EntryPtr = 0;
658 break;
659 }
660 }
661 PrevOffset = NextEntryOffset;
662 while (PrevOffset != 0) {
663 return ((ULONG)UserBuffer & 1); // over byte ptr [ebp+UserBuffer+3], 0, / word, al
664 }
```

תודה רבה !

