02 אפריל 2015

י״ג ניסן תשע״ה

סימוכין : י-ס- 090

הנדון: התרעה אודות מערך "Volatile Cedar"

רקע:

חברת Check Point פרסמה דו״ח אודות מערך תקיפה מתוחכם המכונה "Volatile Cedar". חברות אבטחת מידע נוספות, ביניהן FireEye ו-Kaspersky, פרסמו התייחסות למערך זה בהפניה לפרסום של חברת Check Point. מערך זה תוקף שרתי WEB ובאמצעותם מתקין פוגען פרי פיתוח עצמי (המכונה Explosive) לתקיפת ארגונים שונים ברחבי העולם, כולל ארגונים הקשורים לישראל.

שלבי התקיפה:

1. ביצוע סריקת חולשות על שרתי WEB בעלי תשתית ASPX על מנת למצוא נקודות כניסה לארגון הנתקף.
2. השתלת WEB SHELL על שרת ה-WEB שאותר כפגיע.
3. ביצוע מיפוי תצורה וסריקת חולשות של הרשת הפנים-ארגונית באמצעות WEB SHELL.
4. השתלת פוגען המכונה Explosive Trojan, המאפשר לתוקף שליחת פקודות לביצוע וגניבת מידע מהשרת הנתקף דרך מערך של שרתי פיקוד ושליטה.

   במקרים בהם נדרשת תעבורת רשת גדולה בין התוקף לקורבן, התוקף מתקין לקוח PLink על השרת הנתקף שיתקשר אל שרתי SSH של התוקף.
5. תיאור הפוגען Explosive Trojan :
   א. הפוגען נפוץ בחמש גרסאות וכולל שני סוגי קבצים :
      1) הפוגען עצמו - קובץ exe.
      2) הרחבה של יכולות הפוגען - קובץ dll.
   ב. יכולות הפוגען :
      1) ניטור הקשות מקלדת (Key Logger).
      2) ניטור לוח עריכה (Clipboard Logger).
      3) ניטור ניצולת הזיכרון של הפוגען.

4) התפשטות להתקני זיכרון נתיקים.

5) התקשרות מאובטחת מול שרתי פיקוד ושליטה:

i. הפסקת תעבורה בשעות בהן אין פעילות.

ii. בדיקה של זמינות השרת והרשת.

iii. עדכון כתובות של שרתי הפיקוד והשליטה.

iv. העברת מידע בצורה מקודדת (בחלק מהגרסאות).

אינדיקטורים (IOC)

(Indicators Of Compromise) - מאפיינים שנצפו ברשת או במערכת ההפעלה שעשויים להעיד על חדירה או פגיעה במערכות מחשב.

להלן החתימות הידועות ושרתי ה-C&C שנצפו בתקיפות נוספות:

(יתכן שחתימות מסוימות לא יופיעו כלל עקב אי הפעלת שלב מסוים, או עקב שינוי בשמות הקבצים, יתכן אף כי גם כתובות ה- IP של שרתי ה-C&C משתנות ואינן הכתובות שנצפו בתקיפות שהתגלו)

Network IOC:

IP:

- 69.64.90.94
- 50.60.129.74
- 85.25.20.27
- 213.204.122.133
- 184.107.97.188
- 50.60.129.78
- 69.94.157.80
- 213.204.122.130

Domains:

- saveweb.wink.ws
- carima2012.site90.com
- explorerdotnt.info
- dotnetexplorer.info
- dotntexplorere.info
- xploreredotnet.info
- erdotntexplore.info

C&C paths:

- /ex/ie.php
- /445/ie.php
- /microsoft/ie.php
- /microsoft/index.php
- /80/index.php
- /443/index.php
- /445/index.php
- /v2/443/index.php
- /v2/445.index.php
- /v2/p5/80/index.php
- /v2/p5/443/index.php
- /v2/p5/445/index.php
- /v2/p3/80/index.php
- /v2/p3/443/index.php
- /v2/p3/445/index.php
- /v3/80/index.php
- /v3/443/index.php
- /v3/445/index.php

TCP Payloads:

- ==gKg5XI+BmK
- <*`!Q@W#E4'*>
- <'|'>Explosive

HTTP Values:

User Agent	Mozilla/4.0 (compatible; MSIE 7.0; MSIE 6.0; Windows NT 5.1; .NET CLR 2.0.50727)
URL Contains	php?win=1
URL Contains	php?win=4
URL Contains	Php?micro=
GET Request Contains	GET//

C&C Commands:

- '==gKg5XI+BmKqwUazRHUy92YlN3c'
- ==gKg5XI+BmKqsUasxGUy92YlN3c
- ==gKg5XI+BmKqIVduNUbkpCf
- ==gKg5XI+BmK==gKF5WdttUZ5NnK
- ==gKg5XI+BmK=oSRuVXbS92b0tUZ5NnK
- ==gKg5XI+BmK==gKHVGdSV2ZWFGb1VmK
- ==gKg5XI+BmKqQVZs5WZ0pCP
- ==gKg5XI+BmKqEEZkRUaypCP
- ==gKg5XI+BmKqQUZsRUaypCP
- ==gKg5XI+BmK==gKHVGdEJXa2V2cG9GbkVmc
- ==gKg5XI+BmKqcUZ0RkcpZXZzpCP
- ==gKg5XI+BmKqcUZ0ZUasVmK
- ==gKg5XI+BmK=oyUjNFavRnK
- ==gKg5XI+BmK==gKEVXbwBVYzNnK
- ==gKg5XI+BmK==gKEVXbwhUazRnK
- ==gKg5XI+BmK=oySllHTvdmK
- '==gKg5XI+BmK=wTIqIVRSVlTqEiP
- ==gKg5XI+BmK==APhoySJxETqEiP
- ==gKg5XI+BmK8EiKEVETqEiP
- ==gKg5XI+BmK8oCYF9kRgpiP
- ==gKg5XI+BmK=wTlqaqEiP
- ==gKg5XI+BmK=oSVupVawpCP
- ==gKg5XI+BmKqwUazRHUy92YlN3c
- ==gKg5XI+BmKq8Ecl5GUGpyW
- ==gKg5XI+BmK==gKqMEbvNXZGlGblpiK
- ==gKg5XI+BmK=oiRpxWZTVmbkpCP
- ==gKg5XI+BmK=oyQslGci9WYyRGTvdmK
- ==gKg5XI+BmK==gKF5WdtdVauR2b3NnK
- ==gKg5XI+BmK=oCRlxWZ0VmRpxWZzpCP
- ==gKg5XI+BmK=oyQvBXeQF2c0VmRpxWZzpCP
- ==gKg5XI+BmK==gKDVHdQF2c0VmRpxWZzpCP
- ==gKg5XI+BmKqoVawpCP

Host IOC:

Services:

- Helper
- WindowsHelper
- VMWareActivationHelper
- WindowsInet
- WindowsHelpService
- WindowsHelpServices
- WindowsInetService
- MicrosoftIserv
- MicrosoftServices
- MicrosoftSystemClock

Web Shell Files:

- 404.asp
- 404.aspx
- Caterpillar.aspx
- Heblib140201.aspx

Files:

- aqagent.exe
- vsmss.exe
- qsagent.exe
- w3wp.exe
- cvsc.exe
- whelp.exe
- dllhost.exe
- whttpd.exe
- dllvhost.exe
- winet.exe
- dwcm.exe
- winhelp.exe
- embedded.exe
- winhlp.exe
- ieservice.exe
- winhttpd.exe
- logsys.exe
- wininet.exe
- nsp.exe
- winlog.exe
- rundll32.exe
- winscr.exe
- sccsc.exe
- winscrv.exe
- whelp.exe
- vmtools.exe
- whttpd.exe
- vmtoolsd.exe
- vsystem.dll
- winsec.dll
- tools.dll
- serverhelp.dll
- wnhelp.dll
- %temp%\systmp.dat
- %temp%\systmp2.dat
- svskey.exe
- svchost.exe
- wnhelp.exe
- syslog.exe
- wnsys.exe
- syswin.exe
- wshelp.exe
- updater.exe
- wvsys.exe
- vmacthlpsrv.exe
- winserv.exe
- svsc.exe
- wisrv.exe
- %systemroot%\Microsoft Help\Secure\wintc\
- %systemroot%\Microsoft Help\Secure\wintp\%username%-%date.time%.dat
- %systemroot%\Microsoft Help\Secure\wintc\%username%-%date.time%.dat
- c:\recycler\Microsoft Help\Secure
- c:\recycler\Microsoft Help\Secure\%username%.tp.dat
- c:\recycler\Microsoft Help\Secure\%username%.tc.dat
- c:\recycler\Microsoft Help\Secure\wintp\
- c:\recycler\Microsoft Help\Secure\wintc\
- c:\recycler\Microsoft Help\Secure\wintp\%username%-%date.time%.dat
- c:\recycler\Microsoft Help\Secure\wintc\%username%-%date.time%.dat
- [CurrentRunningFolder]\%username%-rpt.sys
- [CurrentRunningFolder]\%username%-crpt.sys
- [CurrentRunningFolder]\winrpt
- [CurrentRunningFolder]\wincrpt

- [CurrentRunningFolder]\winrpt\%username%-%date.time%.sys
- [CurrentRunningFolder]\wincrpt\%username%-%date.time%.sys
- %systemroot%\Microsoft Help\Secure
- %systemroot%\Microsoft Help\Secure\%username%.tp.dat
- %systemroot%\Microsoft Help\Secure\%username%.tc.dat
- %systemroot%\Microsoft Help\Secure\wintp\

Explosive's Installed Paths:

- %systemroot%
- %systemroot%\system32
- %systemroot%\SysWOW64
- %appdata%
- %programfiles%\VMware\VMware Tools
- %programfiles%\VMWare\VMware Tools\win32
- %programfiles%\Notepad++

MD5:

- 44db62acf787be73dcf8968d360f32b8
- 9f98eb473d3723f09d6a94cb326d4984
- dab2cbb34ec587587bdf0418f7fb06b1
- d028eacd721e0b2d6e9ce19d2575d51b
- eb7042ad32f41c0e577b5b504c7558ea
- 44b5a3af895f31e22f6bc4eb66bd3eb7
- 08c988d6cebdd55f3b123f2d9d5507a6
- 61b11b9e6baae4f764722a808119ed0c
- c7ac6193245b76cc8cebc2835ee13532
- 184320a057e455555e3be22e67663722
- 5d437eb2a22ec8f37139788f2087d45d
- 1dcac3178a1b85d5179ce75eace04d10
- 9a5a99def615966ea05e3067057d6b37
- 2b9106e8df3aa98c3654a4e0733d83e7
- ab3d0c748ced69557f78b7071879e50a
- c9a4317f1002fefcc7a250c3d76d4b01
- 4f8b989bc424a39649805b5b93318295
- 3f35c97e9e87472030b84ae1bc932ffc
- 7cd87c4976f1b34a0b060a23faddbd19
- f58f03121eed899290ed70f4d19af307
- 96b1221ba725f1aaeaaa63f63cf04092
- ea53e618432ca0c823fafc06dc60b726
- 034e4c62965f8d5dd5d5a2ce34a53ba9
- 5ca3ac2949022e5c77335f7e228db1d8
- 306d243745ba53d09353b3b722d471b8
- e6f874b7629b11a2f5ed3cc2c123f8b6
- 5b505d0286378efcca4df38ed4a26c90
- 7dbc46559efafe8ec8446b836129598c
- 1d4b0fc476b7d20f1ef590bcaa78dc5d
- 66e2adf710261e925db588b5fac98ad8
- c898aed0ab4173cc3ac7d4849d06e7fa
- 22872f40f5aad3354bbf641fe90f2fd6
- c19e91a91a2fa55e869c42a70da9a506
- 740c47c663f5205365ae9fb08adfb127
- edaca6fb1896a120237b2ce13f6bc3e6
- d2074d6273f41c34e8ba370aa9af46ad
- 6f11a67803e1299a22c77c8e24072b82
- 7031426fb851e93965a72902842b7c2c
- 981234d969a4c5e6edea50df009efedd
- 2783cee3aac144175fef308fc768ea63
- 29eca6286a01c0b684f7d5f0bfe0c0e6
- 826b772c81f41505f96fc18e666b1acd

YARA rules:

1.

```
rule explosive_exe
{
   meta:
      author = "Checkpoint Software Technologies inc."
      info = "Explosive EXE"
  strings:
      $MZ = "MZ"
      $DLD_S = "DLD-S:"
      $DLD_E = "DLD-E:"
  condition:
      $MZ at 0 and all of them
}
```

2.

```
import "pe"
rule explosive_dll
{
    meta:
       author = "Checkpoint Software Technologies inc."
       info = "Explosive DLL"
    condition:
       pe.DLL
       and ( pe.exports("PathProcess") or pe.exports("_PathProcess@4")
       and pe.exports("CON")
}
```

Explosive's Strings:

- DLD-ACT
- DLD-C
- DLD-C0
- DLD-D
- DLD-E
- DLD-P
- DLD-IHC
- DLD-USA
- DLD-IP
- DLD-OIP
- DLD-NTI
- DLD-RCH
- DLD-RL
- DLD-RN
- DLD-S
- DLD-IH1
- DLD-IH2
- DLD-PRT
- DLD-USI
- DLD-SN
- DLD-ST
- DLD-TN

Exported DLL Function:

- CON
- GetAllData
- GetIEHistory
- OpenClipFn
- PathProcess
- SetWinHoK
- Registerapp
- CreateNewFile
- Fdown

Removable Device IOC:

שמות הקבצים מופיעים לעיתים גם עבור קבצים לגיטימיים במדיה נתיקה.

- `autorun.exe`
- `Autorun.inf`

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר.

לכל מידע נוסף ניתן לפנות אלינו.

הערה: שיתוף מידע עם ה- CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כל שהוא, במידה שהתגלה צורך כזה.

בברכה,

CERT-IL

טל: 03-7450801

team@cert.gov.il