05 יולי 2015

י״ח תמוז תשע״ה

סימוכין : י-ס- 134

הנדון: התרעה על וריאנט חדש של הפוגען Zeus

תיאור

לאחרונה הגיע לידי ה-CERT הלאומי מידע על גל תקיפה רחב של וריאנט חדש של הפוגען Zeus (אשר לרוב משמש למטרות גניבת מידע פיננסי). הפוגען מתפשט באמצעות מייל דיוג בצירוף קישור המפנה לכתובת הגורמת להדבקה.

תהליך התקיפה

1. המייל נשלח בצירוף קובץ doc. זדוני אשר עושה שימוש בחולשה ידועה לשם הורדת הפוגען.
2. בעת פתיחת הקובץ הזדוני, מתבצעת פנייה לכתובת לגיטימית `yandex.ru` על מנת לבדוק האם המחשב מחובר לרשת האינטרנט. במידה והמחשב מחובר לרשת האינטרנט, מתבצעת פנייה לצורך הורדה והתקנה של הפוגען.
3. לאחר ההתקנה הפוגען מפיץ את עצמו לרשימת אנשי הקשר בדוא״ל המחשב הנתקף.
4. הפוגען מאפשר לתוקף יכולת שליטה מלאה מרחוק על המחשב הנתקף.

מזהים (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 וחתימות 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)

כתובות IP :

- 85.25.100.75
- 41.204.128.242
- 179.43.128.238
- 95.134.107.123
- 213.180.204.3
- 109.108.143.46

Domains:

- previewproperty.co.uk
- shiraland.su
- yandex.ru
- Krutobruto.su

תיקיות וקבצים (Files):

- %temp%\tmp[random]
- signons2.exe
- %temp%\tmp5cd74bbf.bat
- %temp%\tmp9d21da33\winsrc.exe
- C:\Users\%username%\Local Settings\Temporary Internet Files\Content.IE5\KNOKM7UC\31223122[1].exe
- %appdata%\winicsve.exe
- 31223122.doc
- Bot.exe
- Tmpeaff1584.exe
- Sail[random].jpg
- Agent.exe
- Bot_secondsample.exe
- Mp3_file_kanye_west.mp3

מזהי Cookie:

- %username%\yandex[1].txt

מזהי MD5 שנמצאו:

- A93CFE3FA538C86F41D448E426ECCBD2
- B5EA485DC4247D944736DFF62BA4D668
- B1877E564A21BCB3EE9F3903E7A14710
- 46444B8C103B65FBD85002F2221BEA3F
- bdd76cf3b4bad8062166f72c7014aca7
- 01be04b5e66966abeef8da0420f40d3a
- 7f1bcd2c08a32cfc272a585df3a35142
- 1eeb17e0a3a5e4083aa813c779fa55d3
- D7af1afe9d76b732cc1aa5aa5c686104
- 4d77d9fa99fdb0f348809ca1b051bbc8
- 07b4faf3972287e72fc5ad03f285fda2

מזהי SHA-1 שנמצאו:

- 44bbb4fc2da6c5c7c4b32779dc94f8b020b866fe
- 0142e694dfbaa33a5cae3eccc8c305bab6dbee8c
- 464e4b26b2713f161a154197c9d694561de66b9f

מזהי SHA-256 שנמצאו:

- 20b37e3df8656b76130a766554d0de6248b10c367a1b4ed7722642fd81ac2fff
- ade69aaff3ef30a94693a0640303e508fbd4a97d58ccd566d9f79562361f40ab
- 6c2fbbc2a2e266225cc844db16c3cad8be1b13acb03c844d0ca4b19cf34ef439

מזהי SHA-512 שנמצאו:

- 0d8a115f16cf1e7ed41175815e451b42f7487d15bbfcd2fabba497629f5971453bd45c51726c52e072a842fd33c30fa6dbeef9807f516b80f8e734b0dae77c42
- 9cc36ea47950df8747b4927cda14a5006c16bac393c4619e19c3d3d4a1cee5fe379e50ae5dd0823b9a262db4dfbc8173009e2a8c0aab233d866491971fc497b7
- f645c2db31e5eb428187ecf929f6e6d6fb48b7578450df397644abb14f69899345b2bf4294f2a6a37862dd8bb3a5b662ae765f4afd05203a4d1b7627212b7aaf

חתימות YARA:

```
rule CERT-IL-ALERT-A-C-134
{
meta:
      author = "CERT-IL"
      date = "2015-07-05"
      description = "Zbot-Detection"
      hash0 = "b5ea485dc4247d944736dff62ba4d668"
      hash1 = "b1877e564a21bcb3ee9f3903e7a14710"
      sample_filetype = "exe"
strings:
      $string0 = "LWh@yB"
      $string1 = "HtYHt6H"
      $string2 = "V@W@PQ"
      $string3 = "Bjjjjjj" wide
      $string4 = "Bjjjjj" wide
      $string5 = "Bjjjjjjjjj" wide
      $command1 = "cmd=PING" wide
      $command2 = "cmd=xpay&who=" wide
condition:
       5 of ($string*) or 2 of ($command*)
}
```

חתימות Snort:

- `alert tcp any any -> any 80 (msg:"CERT-IL-ALERT-A-C-134"; flowbits:isnotset, httprequest; content:"GET"; http_method; content:"Accept: */*"; http_header; content:"img.php?id="; http_uri; flowbits:set, httprequest; classtype:beaconing-medium-confidence; priority:3; gid:666; sid:12616; rev:2;)`

- `alert tcp any any -> any 80 (msg:"Zeus TROJAN Downloader"; flowbits:isnotset, httprequest; content:"GET"; http_method; content:"Accept: */*";http_header; content:"/zecmd/"; http_uri; flowbits:set, httprequest; classtype:beaconing-medium-confidence; priority:3; gid:666; sid:12616; rev:2;)`

- `alert tcp any any -> any 80 (msg:"Zeus Trojan C&C Beaconing"; content:"/gate.php"; content:"POST"; http_method; classtype:beaconing-medium-confidence; priority:3; gid:666; sid:12616; rev:2;)`

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