DEEPCYBER

Advanced Intelligence, Protection, Antifraud.

CYBER THREAT INTELLIGENCE REPORT
PETYA-BASED RANSOMWARE

Revision n. 01, Revision Data: 27.06.2017, Risk Level: HIGH, TLP: WHITE

TABLE OF CONTENTS

Contents

Executive Summary

L'obiettivo del report è quello di fornire le prime informazioni relative all'infezione su larga scala, derivante dalla diffusione di un *ransomware* basato su una variante del codice Petya.

La prima segnalazione dell'attacco è avvenuta intorno alle 12:00 GMT+1 del 27.06.2017.

Diverse fonti convergono verso l'ipotesi che il vettore di attacco inizialmente utilizzato per la diffusione dell'infezione sia legato ad un aggiornamento infetto per la suite software MeDoc, un pacchetto software utilizzato da molte organizzazioni ucraine.

A livello locale, l'infezione si propaga sfruttando la vulnerabilità CVE-2017-0199 (detta *EternalBlue*) e, in particolare, una versione modificata dello stesso exploit impiegato nel ransomware *WannaCry*.

La vulnerabilità EternalBlue è legata al protocollo SMB utilizzata sui sistemi Microsoft da Windows XP a Windows 2008 sulla porta TCP 445 o 139 a cui non è stata precedentemente applicata la patch Microsoft MS17-010.

Il ransomware utilizza anche le utility Psexec e WMI (Windows Management Instrumentation) che sono componenti lecitamente presenti nei sistemi Windows. Secondo l'analisi svolta da Group IB, il malware sfrutta anche la vulnerabilità CVE-2017-0144.

Sebbene siano state registrate decine di migliaia gli attacchi informatici legati a questa infezione, i principali target sono aziende localizzate in Ucraina, Russia ed Europa Occidentale e appartenenti a diversi *industry* quali ad esempio terminal portuali, aeroporti, aziende energetiche, banche, fabbriche, società di assicurazioni, servizi militari.

Descrizione dell'incidente / infezione

L'Attaccante (o il gruppo di attaccanti) dietro la campagna di diffusione del codice malevolo basato su Petya sta ottenendo l'accesso ai server di diverse aziende principalmente localizzate in Ucraina, Russia ed Europa Occidentale.

Breve descrizione della tipologia dell'infezione

Il tipo codice malevolo utilizzato per l'infezione dei sistemi informativi è un ***ransomware***. Un ransomware è un malware che impedisce o limita agli utenti di accedere al loro sistema sia bloccando schermo del sistema o bloccando i file degli utenti attraverso la cifratura di tutti i file o dei file aventi una determinata estensione (ad es. doc/docx; xls/xlsx; etc).

La propagazione nelle reti locali avviene attraverso il protocollo Remote Desktop Protocol (RDP) sfruttando la vulnerabilità critica legata al Windows SMB vulnerability (MS17-010).

L'analisi codice ha determinato che l'infezione fa uso dei comandi WMI e PSExec come *lateral movement* per propagarsi su altri sistemi.

L'analisi di dettaglio del codice è ancora in corso e maggiori dettagli saranno forniti non appena disponibili.

Da quanto fino a questo momento stabilito, il codice malevolo si sta diffondendo attraverso due campioni che possiamo distinguere sulla base del loro valore hash (in particolare SHA-256):

1. 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
2. 64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1

Alcuni dei nomi associati ai file infetti che sono i seguenti:

- some ransomware.exe
- svhost.exe
- perfc.dat
- ran.exe
- Petyav2 - Maybe.bin
- petya.exe
- 027cc450ef5f8c5f653329641ec1fed9.exe
- petwrap.exe

- petrcrpt.exe
- 71b6a493388e7d0b40c83ce903bc6b04.bin
- 222068554
- samplespetya.exe
- PetyaWrap.dll

I due campioni, rispettivamente, hanno le seguenti caratteristiche:

MD5: 71b6a493388e7d0b40c83ce903bc6b04

SHA-1: 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d

SHA-256: 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745

Imphash: 52dd60b5f3c9e2f17c2e303e8c8d4eab

Size: 353.9 KB (362360 bytes)

Type: Win32 DLL

Signing date: 11:52 PM 6/27/2017

Entry Point: 0x00007D39

Compilation timestamp: 2017-06-18 07:14:36

MD5: e285b6ce047015943e685e6638bd837e

SHA-1: 9717cfdc2d023812dbc84a941674eb23a2a8ef06

SHA-256: 64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1

Imphash: 52dd60b5f3c9e2f17c2e303e8c8d4eab

Size: 353.9 KB (362360 bytes)

Type: Win32 DLL

Signing date: 9:57 PM 6/27/2017

Entry Point: 0x00007D39

Compilation timestamp: 2017-06-18 03:13:01

La data di compilazione è confermata dall'analisi del codice:

```
.rdata:10015510 ; Export directory for perfc.dat
.rdata:10015510 ;
.rdata:10015510                 dd 0                    ; Characteristics
.rdata:10015514                 dd 5945EFBCh            ; TimeDateStamp: Sun Jun 18 03:13:00 2017
.rdata:10015518                 dw 0                    ; MajorVersion
.rdata:1001551A                 dw 0                    ; MinorVersion
.rdata:1001551C                 dd rva aPerfc_dat       ; Name
.rdata:10015520                 dd 1                    ; Base
.rdata:10015524                 dd 1                    ; NumberOfFunctions
.rdata:10015528                 dd 0                    ; NumberOfNames
.rdata:1001552C                 dd rva off_10015538     ; AddressOfFunctions
.rdata:10015530                 dd 0                    ; AddressOfNames
.rdata:10015534                 dd 0                    ; AddressOfNameOrdinals
```

Elementi significativi presenti nel codice sorgente e legati all'ottenimento del riscatto sono i seguenti:

- ✓ all'indirizzo esadecimale 1001AB26 000001FF è presente la seguente stringa col valore del riscatto richiesto: *"If you see this text, then your files are no longer accessible, because they\r\n have been encrypted. Perhaps you are busy looking for a way to recover your\r\n files, but don't waste your time. Nobody can recover your files without our\r\n decryption service.\r\n\r\n We guarantee that you can recover all your files safely and easily. All you\r\n need to do is submit the payment and purchase the decryption key.\r\n\r\n Please follow the instructions:\r\n\r\n 1.* ***Send $300*** *worth of Bitcoin to following address:\r\n \r\n"*
- ✓ all'indirizzo esadecimale 1001AD2C 00000090 è presente la seguente stringa con l'indirizzo di posta elettronica a cui inviare il proprio Bitcoin wallet ID*: "\r\n\r\n 2. Send your Bitcoin wallet ID and personal installation key to e-mail\r\n* ***wowsmith123456@posteo.net****. Your personal installation key:\r\n\r\n"*
- ✓ all'indirizzo esadecimale 1000FF88 00000023 è presente la seguente stringa con l'indirizzo bitcoin a cui inviare il riscatto: "***1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX***".

- ✓ L'indirizzo di posta elettronica wowsmith123456@posteo.net è stato già bloccato nella giornata odierna come comunicato dal sito di Posteo (https://posteo.de/en/blog/info-on-the-petrwrappetya-ransomware-email-account-in-question-already-blocked-since-midday) su cui era stata registrato l'account utilizzato per chiedere il riscatto.

Informazioni di dettaglio sulle transazioni operate sull'indirizzo bitcoin 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX (ed avente Hash-160 e62f3c2c154063f3e230d293701c7583f5489556) presente nel codice sorgente del ransomware sono disponibili all'indirizzo web:

- ✓ https://blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

Al momento della scrittura del presente report lo stato delle transazioni verso questo indirizzo è mostrata dalla seguente figura:

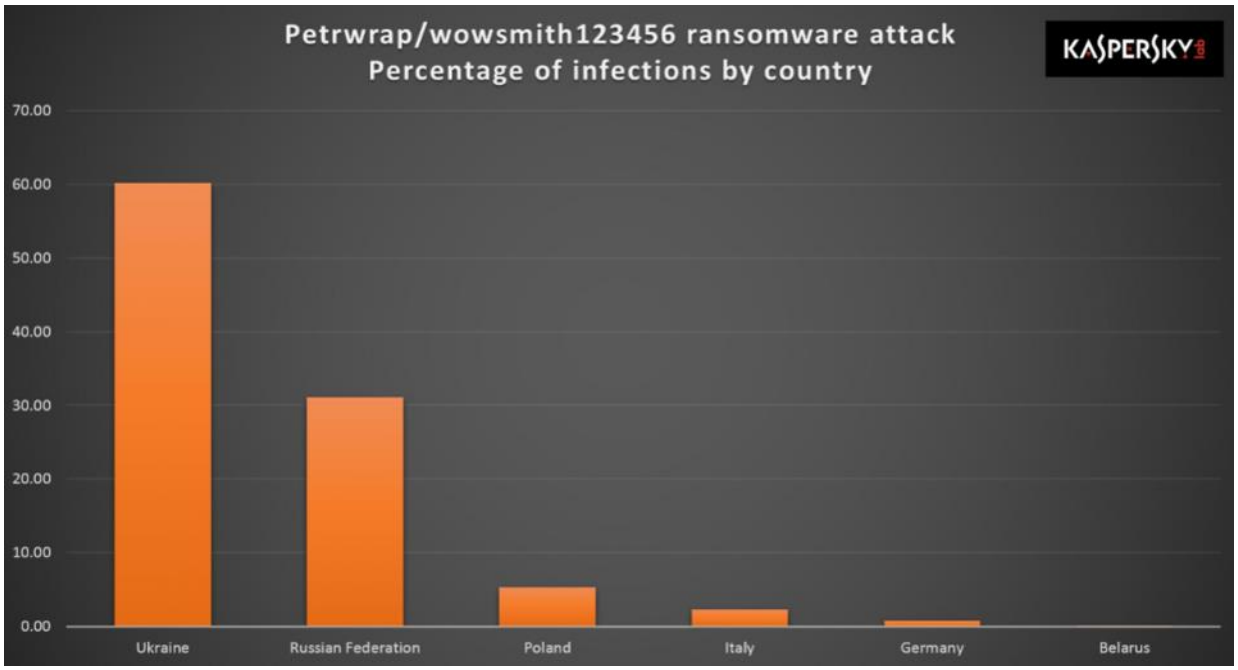
SISTEMI IMPATTATI DALL'INCIDENTE

I sistemi impattati dall'infezione sono i sistemi Microsoft da Windows XP a Windows 2008 su cui è abilitato il servizio SMB sulla porta 445 e a cui non è stata precedentemente applicata la patch Microsoft MS17-010

DIFFUSIONE DELL'INFEZIONE GEO/TIME BASED

La prima segnalazione dell'attacco è avvenuta intorno alle 12:00 GMT+1 del 27.06.2017 è compatibile con la segnalazione che l'azienda Medoc (www.medoc.ua) ha inviato sulla pagina facebook https://www.facebook.com/medoc.ua/posts/1904044929883085.

Secondo gli analisti della società Kaspersky, la diffusione geografica dell'infezione ha colpito principalmente l'Ucraina e la Russia come si può osservare dalla figura seguente:



Dettagli tecnici dell'infezione

COMPORTAMENTO DELL'INFEZIONE

Il ransomware, una volta presente su un nuovo sistema, elenca tutti gli adattatori di rete, tutti i nomi dei server conosciuti tramite NetBIOS e recupera, attraverso una scansione, gli indirizzi (se disponibili) DHCP forniti ai sistemi della rete locale.

Per ogni indirizzo IP della rete locale viene verificata lo stato delle porte TCP aperte 445 e 139 per accertare se queste sono aperte. Successivamente, le macchine su cui sono trovate le porte utilizzate dai protocolli vulnerabili sono attaccate con uno dei metodi descritti in precedenza o sfruttando le vulnerabilità CVE-2017-0144, CVE-2017-0199 (secondo la fonte Group IB) e i comandi Psexec e WMI.

Dopo che un sistema viene infettato, il malware modifica l'MBR e l'MFT sul computer e pianifica il suo riavvio. Una volta che il sistema si riavvia, appare all'utente un falso messaggio legato all'utility "chkdisk" e viene avviata la cifratura basata sull'algoritmo RSA a 2048-bit dei file di interesse del malware.

I file presenti sul disco che saranno cifrati dal ransomware sono tutti quelli con le seguenti estensioni:

3ds,7z, accdb, ai, asp, aspx, avhd, back, bak, c, cfg, conf, cpp, cs, ctl, dbf, disk, djvu, doc, docx, dwg, eml, fdb, gz, h, hdd, kdbx, mail, mdb, msg, nrg, ora, ost, ova, ovf, pdf, php, pmf, ppt, pptx, pst, pvi, py, pyc, rar, rtf, sln, sql, tar, vbox, vbs, vcb, vdi, vfd, vmc, vmdk, vmsd, vmx, vsdx, vsv, work e xls.

Il commando *Psexec* è utilizzato per eseguire le seguenti istruzioni:

C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1

Analogamente, il commando WMI è utilizzato per eseguire il seguente commando sulla base delle credenziali (precedentemente 'catturate' dal malware) dell'utente del sistema:

Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1"

Infine, il malware cancella le tracce delle operazioni svolte eseguendo i seguenti comandi:

wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:

YARA SIGNATURES

Dall'analisi effettuata si conferma la correttezza e si consiglia l'impiego della seguente regola Yara per l'individuazione del ransomware Petya-Based:

```
rule ransomware_PetrWrap {
meta:
        copyright= "Kaspersky Lab"
        description = "Rule to detect PetrWrap ransomware samples"
        reference = "https://securelist.com/schroedingers-petya/78870/"
        last_modified = "2017-06-27"
        author = "Kaspersky Lab"
        hash = "71B6A493388E7D0B40C83CE903BC6B04"
        version = "1.0"
strings:
        $a1 =
"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2
JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcqYLIBZzQ2ZTK0A2DtX4GRK
xEEFLCy7vP12EYOPXknVy/mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgqCXsPwfITDbDDmdrRIi
UEUw6o3pt5pNOskfOJbMan2TZu" fullword wide
        $a2 =
".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.
```

```
        gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.
        tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls" fullword wide

        $a3 = "DESTROY ALL OF YOUR DATA PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED"
        fullword ascii

        $a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii

        $a5 = "wowsmith123456posteo.net." fullword wide

condition:

        uint16(0) == 0x5A4D and filesize < 1000000 and any of them  }
```

Soluzioni / Raccomandazioni

- Applicare immediatamente le patch per la vulnerabilità MS17-010 SMB e implementare i consigli operativi proposti nei link seguenti:
  - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  - https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows
  - https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx?utm_campaign=Petya%2FNotPetya%20Ransomware%20Prospect%20Email%20-%206.27&utm_medium=email&utm_source=Eloqua

- Creare il *killswitch* legato a questo ransomware creando un file con nome *perfc.dat* nella cartella C:\Windows\

- Avviare una attività di scansione dei dischi locali e delle cartelle di rete condivise (anche utilizzando la regola Yara prima riportata) al fine di ricercare eventuali presenze di codice malevolo. Anche nel caso in cui non fosse stata rilevata la presenza di minacce; definire un piano di scansioni da eseguire su base regolare temporale.

Anche se lo stato attuale dell'analisi non ha permesso di stabilire ancora tutti i meccanismi di propagazione su Internet e gli stage realizzati nel corso dell'infezione, si ritiene ragionevole svolgere anche le seguenti attività:

- Verificare il livello dei privilegi associati ad ogni account e implementare il principio di *least privilege*. I diritti di Administrator devono essere forniti (e utilizzati) solo in casi assolutamente

necessari. Allo stesso modo devono essere verificati i diritti di lettura/scrittura soprattutto per le cartelle di rete condivise o quelle in cui sono memorizzati file rilevanti o sensibili.

- Disabilitare l'esecuzione automatica degli script e, in ogni caso, non aprire alcuna email (eventualmente sfuggita al controllo degli apparati di controllo) se non certi del mittente.

- Abilitare un filtro sui sistemi di controllo anti-spamming/phishing e applicare un controllo sulle email in ingresso utilizzando tecnologie come il Sender Policy Framework (SPF); il Domain Message Authentication Reporting and Conformance (DMARC) e il DomainKeys Identified Mail (DKIM).

- Verificare che i dati di backup siano sempre disponibili attraverso test realizzati su base regolare di Recovery.

- Sviluppare un adeguato piano di *awareness* a tutti i dipendenti (o consulenti) che devono utilizzare a vario titolo il servizio di posta elettronica o hanno accesso alla rete Internet e Intranet; evidenziando le minacce relative al non corretto e prudente utilizzo dei servizi aziendali di comunicazione

- Implementare dei piani di formazione a tutti i livelli attraverso apposite piattaforme di e-learning utili alla security *awareness*.

Referenze

[1] http://www.cvedetails.com/cve/CVE-2017-0199/

[2] http://www.cvedetails.com/cve/CVE-2017-0144/

[3] https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html

[4] https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762/

[5] http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

[6] https://www.anomali.com/blog/petya?utm_source=hs_email&utm_medium=email&utm_content=53645113&_hsenc=p2ANqtz-8KqKDf4_yIgym5-p6fPR1abHkEXPJ7bge3BimRKvfUE4CFeqFdZFn_ckjvRbysEyQDvxvekWZHIdwpXWHx4GR_CQgbiw&_hsmi=53645113

[7] https://securelist.com/schroedingers-petya/78870/

[8] https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100

[9] https://risksense.com/_api/filesystem/468/EternalBlue_RiskSense-Exploit-Analysis-and-Port-to-Microsoft-Windows-10_v1_2.pdf

[10] https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

DeepCyber Srl

info@deepcyber.it

Piazzale L. Sturzo 15 – 144, ROMA