WannaCry

Storia di un disastro annunciato

Stefano Maccaglia
Malware Researcher

Antefatto

- Cosa dire di un malware che è riuscito a bloccare il servizio sanitario del Regno Unito? Importanti Provider in Europa, nonché molti siti produttivi (vedi Renault)?
- Di chi è la colpa di questo disastro?
- Sicuramente dei Cybercriminali che hanno sviluppato questo malware, ma in questa storia le colpe sono da distribuire tra più soggetti del solito…

Antefatto

- Microsoft in questi giorni sta puntando l'indice verso la National Security Agency perché la vulnerabilità sfruttata dal malware proviene da sue ricerche non divulgate attraverso cui la stessa NSA aveva poi sviluppato una serie di malware.
- In effetti l'idea di sviluppare "zero-day" per finalità di spionaggio può essere sensata, ma nel momento in cui queste vulnerabilità cadono nelle mani di terze parti, che senso ha non divulgarne l'esistenza alle aziende coinvolte, in questo caso Microsoft?
- Per questa ragione, ritengo sia utile avviare una riflessione sull'intera faccenda... partendo dai fatti...

I FATTI

- In Aprile, un gruppo di cybercriminali che si nasconde dietro allo pseudonimo di "Shadow Brokers" ha rilasciato un set di tool trafugati alla National Security Agency.
- Il set contiene tra l'altro il codice di una vulnerabilità nota con il nome di "EternalBlue" (MS17-010), che sfrutta una debolezza in **Microsoft Windows SMB Server** (il servizio di share di file e cartelle) per poter eseguire codice arbitrario da remoto.
- Il rilascio di questo codice era stato anticipato dagli Shadow Brokers mesi prima e i primi leak di documentazione e notizie sulle vulnerabilità poi diffuse risalgono addirittura all'Agosto 2016.

The Equation giveaway

By GReAT on August 16, 2016. 7:22 pm

INCIDENTS

APT | CYBER ESPIONAGE | SHADOW BROKERS | TARGETED ATTACKS | VULNERABILITIES AND EXPLOITS | ZERO-DAY VULNERABILITIES

Rare implementation of RC5/RC6 in 'ShadowBrokers' dump connects them to Equation malware

Confirmed: hacking tool leak came from "omnipotent" NSA-tied group

Rare crypto implementation in ShadowBrokers dump connects it to Equation Group.

DAN GOODIN - 8/16/2016, 11:09 PM

Microsoft Security Bulletin MS17-010

✗ Con un bollettino, pubblicato il 14 Marzo 2017, Microsoft spiega i rischi legati a una vulnerabilità che, se sfruttata, permette la diretta esecuzione di codice arbitrario da remoto, sulla macchina vittima, sfruttando una precisa serie di messaggi verso il servizio di share Microsoft Server Message Block 1.0 (SMBv1).

✗ Il driver **srv. sys** quando processa la funzione **SrvOs2FeaListSizeToNt** in presenza di istruzioni opportunamente manipolate, alloca memoria fuori dei confini originali permettendo l'esecuzione di istruzioni non filtrate dai controlli di sicurezza del Sistema.

```
unsigned int __fastcall SrvOs2FeaToNt(int a1, int a2)
{
int v4; // edi@1
_BYTE *v5; // edi@1
unsigned int result; // eax@1
v4 = a1 + 8;
*(_BYTE *)(a1 + 4) = *(_BYTE *)a2;
*(_BYTE *)(a1 + 5) = *(_BYTE *)(a2 + 1);
*(_WORD *)(a1 + 6) = *(_WORD *)(a2 + 2);
_memmove((void *)(a1 + 8), (const void *)(a2 + 4), *(_BYTE *)(a2 + 1));
v5 = (_BYTE )((_BYTE *)(a1 + 5) + v4);
*v5++ = 0;
_memmove(v5, (const void *)(a2 + 5 + *(_BYTE *)(a1 + 5)),
*(_WORD )(a1 + 6)); //here generates cross-border coverage
result = (unsigned int)&v5[(_WORD *)(a1 + 6) + 3] & 0xFFFFFFFC;
*(_DWORD *)a1 = result - a1;
return result;
}
```

Ops... ci siamo dimenticati qualcosa...

✗ EternalBlue, la documentazione lo evidenziava, permette l'exploit su una vasta quantità di sistemi Microsoft... il problema è che il bollettino MS17-010 non contemplava informazioni circa le machine legacy, in particolare Windows XP...

Operating System	Windows SMB Remote	Windows SMB Remote	Windows SMB Remote	Windows SMB Remote	Windows SMB	Windows SMB Remote	Updates Replaced
Windows 10							
Windows 10 for 32-bit Systems [3] (401260	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	3210720
Windows Vist							
Windows Vista Service Pack 2 (4012598)							
Windows Vista x64 Edition Service Pack 2 (4012598)							
Windows Server 2008							
Windows Server 2008 for 32-bit Systems Service P (401259	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	3177186 in MS16-114
Windows Server 2008 for x64-based Systems Service P (401259							
Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012598)	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	3177186 in MS16-114
Windows Server 2016							
Windows Server 2016 for x64-based Systems [3] (4013429)	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	3213986
Windows 10 Version 1607 for x64-based Systems [3] (4013429)	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	3213986

Windows 7							
Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Only[1]	Critical Remote Code	Critical Remote Code	Critical Remote Code	Critical Remote Code	Important Information	Critical Remote Code	None
Windows 7 for 32-bit Systems Service Pack 1 (4012215)							
Windows 7 for x64-based Systems Service Pack 1 (4012215) Monthly Rollup[1]							
Windows 8.1							
Windows 8. for 32-bit Systems (4012213) Security Only[1]							
Windows 8. for x64-bas Systems (4012216) Monthly Rollup[1]							
Windows Server 2012 and Windows Server 2012 R2							
Windows Server 2012 (4012214) curity ly[1]	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	None
ndows rver 2012 012217) onthly llup[1]	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	3205409
Windows Server 2012 R2 (4012213) Security Only[1]	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	None
Windows Server 2012 R2 (4012216) Monthly Rollup[1]	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	3205401

I Fatti

- Il rilascio del bollettino Microsoft MS17-010, nonostante la sua criticità, non ha avuto l'impatto auspicato. La sua distribuzione e applicazione, inizialmente, non sono state rapide come in altri casi.
- Una ragione è da cercare nella comunicazione, nel senso che ha giocato un ruolo chiave, nel bollettino della Microsoft, il fatto che non venissero citate applicazioni esistenti già capaci di sfruttare questa vulnerabilità, il che ha comportato una diversa considerazione di questa vulnerabilità rispetto a quello che poi si è manifestato.
- Resta importante però sottolineare un elemento essenziale in questo discorso. La NSA non ha divulgato immediatamente, a fronte di un leak di propri documenti e software, le informazioni utili a evitare questo disastro.

I Fatti

- Una parte importante delle colpe della rapida e vasta distribuzione di WannaCry la hanno i vari Dipartimenti IT e i vari Manager che non hanno velocemente implementato la patch fornita a Marzo da Microsoft, ma questo è un malcostume piuttosto diffuso.
- Resta poi da considerare che a fronte di una patch, soprattutto in contesti critici, si attendono le prove di verifica prima di applicarla in ambiti di produzione e questo non può essere considerato sbagliato.
- Come detto… ultimo ma non meno importante, la mancata copertura della patch per XP ha avuto un impatto devastante nelle agenzie pubbliche, specialmente negli ospedali.

WannaCry...

- Ma come si comporta WannaCry...
- Il malware, come altri Ransomware visti in precedenza, critta il Filesystem della macchina vittima e attiva un messagebox in cui chiede un riscatto per "rilasciare" la chiave di decrittazione.
- Il Ransomware è stato sviluppato da cybercriminali, ma non si è ancora definito con precisione il gruppo che lo ha sviluppato e diffuso.
- Al momento (23 Maggio) da verifiche incrociate si è valutato che il malware ha permesso ai cybercriminali di raccogliere non meno di 50.000 Dollari in BitCoint.
- I cybercriminali hanno unito il ransomware con un tool inizialmente sviluppato dall'NSA, che colpisce piattaforme Windows. In questo modo WannaCry ha infettato all'incirca 200,000 computer nel mondo.

Chi è stato danneggiato da WannaCry?

- Il Ransomware, ufficialmente, ha infettato circa 200.000 computer, ma probabilmente il suo numero è di molto superiore in quanto sono noti solo i dati di alcuni paesi (manca ad esempio l'Egitto e la Cina)
- Di certo il malware ha colpito in modo particolarmente virulento il settore dell'Healthcare (ospedali e presidi sanitari pubblici) ove una grande quantità di macchine e PC sono ancora basate su sistemi legacy come Windows XP e non possono essere aggiornate velocemente senza rischiare impatti significativi nella disponibilità dei servizi sanitari ad esse associate.

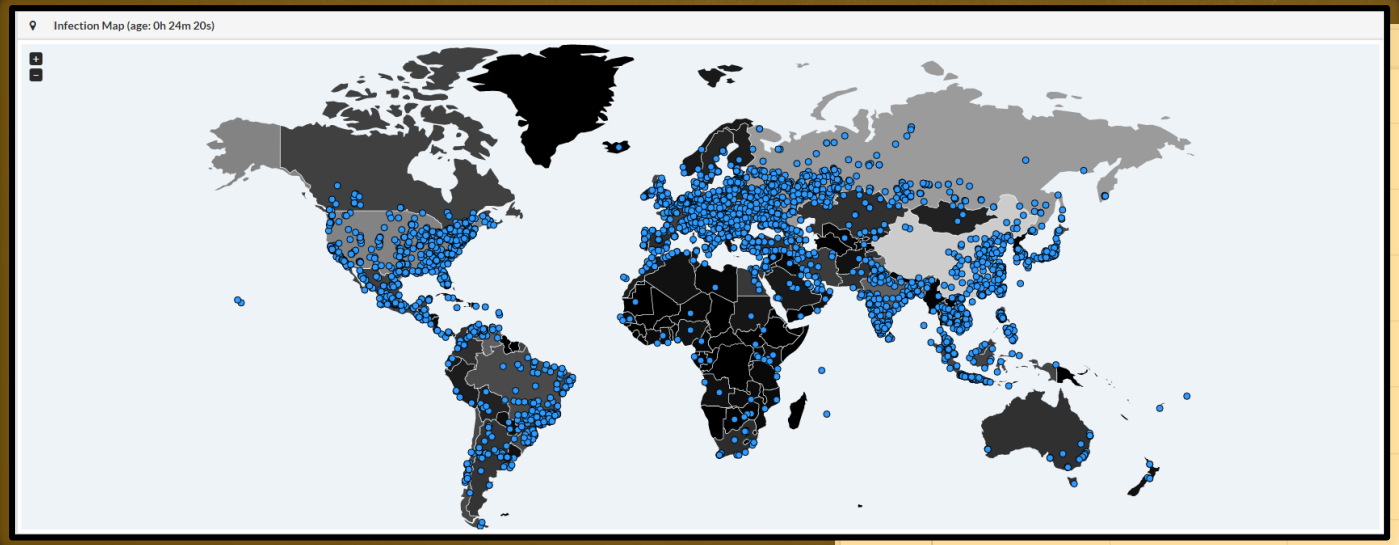
WanaCry Vulnerabilità

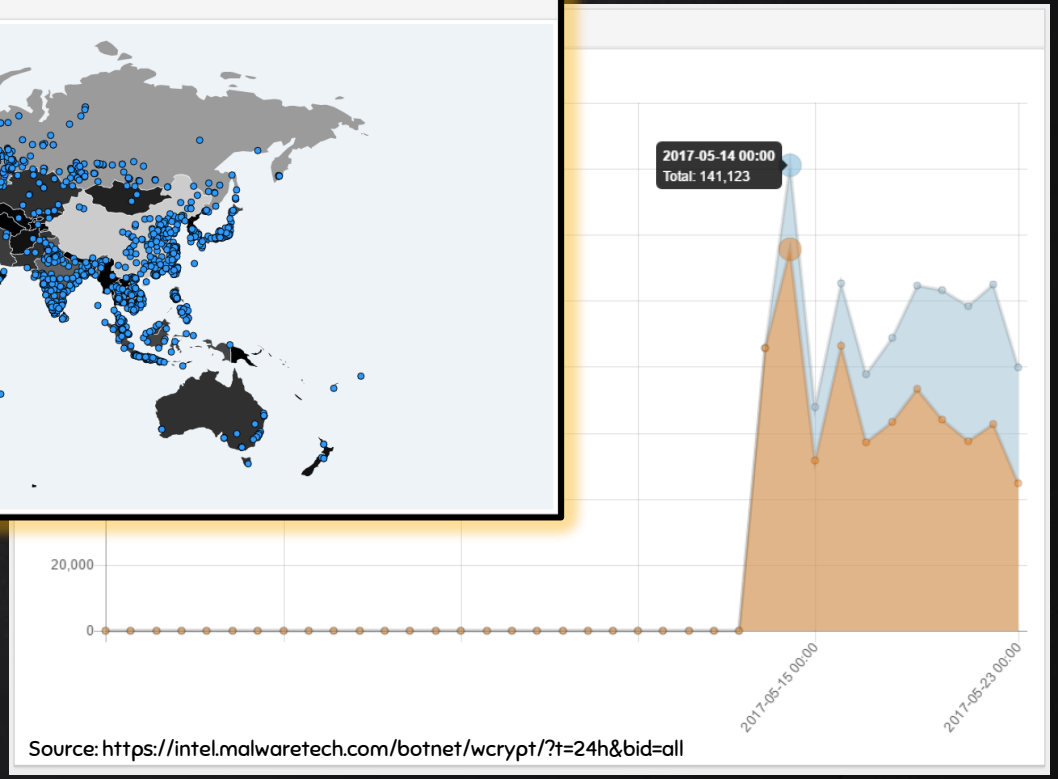
- Come detto, WannaCry sfrutta la vulnerabilità MS17-010 (CVE-2017-0144) per diffondersi in una rete attraverso il protocollo NetBIOS.
- Il malware contiene il codice dell'exploit nel suo codice e lo attiva non appena la prima macchina si è infettata.
- Il principale vettore di diffusione di WannaCry è il protocollo NetBIOS. Anche le email di phishing sono state usate per propagare l'infezione.

WannaCry Ransomware Timeline 2017

Timeline del cyber-attacco

Le conseguenze





Source: https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all

Generazione di IP randomica

✗ In numerosi report abbiamo letto che il ransomware genera una lista di IP interni. Abbiamo riscontrato che il malware genera IP address in modo randomico, non limitandosi solo a quelli privati.

✗ Con questo meccanismo il malware può diffondersi non solo su altre macchine nella stessa rete locale ma potenzialmente anche attraverso Internet. Sempre che il sito target permetta la ricezione di pacchetti NetBIOS da network esterni.

DB349B97...	user-PC	54321	[redacted]	.192.203	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54318	[redacted]	.158.149	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54311	[redacted]	5.237	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54387	[redacted]	.113.121	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54310	[redacted]	35.2	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54309	[redacted]	.134.247	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54306	[redacted]	.0.241	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54305	[redacted]	5.215	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54483	[redacted]	.117.169	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54485	[redacted]	209.232	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54490	[redacted]	.7.193	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54491	[redacted]	.33.170	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54492	[redacted]	2.205	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54494	[redacted]	.212.239	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54495	[redacted]	6.195	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54554	[redacted]	.82.21	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54533	[redacted]	.107.15	445	TCP	SYN Sent	mssecsvc2.0

✗ Questo potrebbe essere un motivo per l'ampia diffusione di questa infezione e anche del perché i ricercatori non sono concordi sul suo vettore iniziale di infezione.

Analisi delle comunicazioni di rete

✗ Un'altra caratteristica interessante del malware è che una volta che rileva una macchina con porta NetBIOS aperta, esso invia tre pacchetti NetBIOS di impostazione sessione. Un pacchetto ha l'IP della macchina che sta tentando di exploitare mentre gli altri due contengono due indirizzi IP "hardcoded" nel codice del malware:

SMB	191	Negotiate Protocol Request
SMB	187	Negotiate Protocol Response
SMB	194	Session Setup AndX Request, User: anonymous
SMB	251	Session Setup AndX Response
SMB	146	Tree Connect AndX Request, Path: \\172.16.99.5\IPC$
SMB	114	Tree Connect AndX Response
SMB	1138	NT Trans Request, <unknown>
SMB	93	NT Trans Response, <unknown (0)>

SMB	191	Negotiate Protocol Request
SMB	187	Negotiate Protocol Response
SMB	194	Session Setup AndX Request, User: anonymous
SMB	251	Session Setup AndX Response
SMB	150	Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB	114	Tree Connect AndX Response
SMB	136	Trans2 Request, SESSION_SETUP
SMB	93	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED

Analisi delle comunicazioni di rete

✗ Le informazione mostrata nel pacchetto seguente mostra l'IP della macchina bersaglio. Si noti l'utilizzo del network di test usato nel nostro laboratorio, 192.168.0.0/24 mentre nella slide precedente abbiamo mostrato gli indirizzi hardcoded:

```
SMB        185 Negotiate Protocol Response
SMB        157 Session Setup AndX Request, User: .\
SMB        175 Session Setup AndX Response
SMB        149 Tree Connect AndX Request, Path: \\192.168.0.1\IPC$
SMB        104 Tree Connect AndX Response
SMB Pip    132 PeekNamedPipe Request, FID: 0x0000
SMB         93 Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
```

Analisi delle comunicazioni di rete – IoC

- Questa caratteristica dell'attività di rete insieme alla presenza dei due indirizzi IP hardcoded (192.168.56.20, 172.16.99.5) può essere usata per scoprire l'exploit attraverso l'utilizzo degli IPS (network intrusion prevention systems).
- I pacchetti SMB (Server message block) contengono inoltre del payload cifrato, che consiste nello shellcode dell'exploit e del file launcher.dll. Nel corso della nostra analisi abbiamo riscontrato che il malware utilizza un algoritmo di cifratura basato su una chiave XOR di 4 byte, 0x45BF6313.

Analisi delle comunicazioni di rete – IoC

- Come riportato da molte fonti, il dropper del malware contiene del codice che esegue un controllo di due specifici domini web prima di eseguire il codice ransomware o il codice di exploit network:

  hxxp://www[dot]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com
  hxxp://www[dot]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com

- Durante la ricerca di ulteriori sample abbiamo rilevato ulteriori altri dropper (MD5: 509C41EC97BB81B0567B059AA2F50FE8) che non esibivano lo stesso comportamento descritto sopra. Questi altri dropper non possiedono neanche il codice di worming via NetBios od il meccanismo di kill switch via domino web. Con questi sample, il codice del ransomware verrebbe esguito in tutti I casi.

Gli Indicatori Di Compromissione – IoC

Dal momento in cui il malware viene lanciato, lascia delle tracce sul filesystem e tramite il meccanismo di "killswitch" verifica se c'e' connessione verso un dominio hardcoded.
Dopodiche' procede tentando l'exploit sul numero maggiore di macchine possibile, in modo da estendere l'infezione.
Contemporaneamente procede a criptare i file sul filesystem e a visualizzare un'applicazione per la verifica del pagamento agli autori.

Filesystem:

- C:\Windows\tasksche.exe
- File che iniziano colla stringa "WANACRY!"
- File con l'estensione ".WNCRY"

Filesystem:

- DNS request to "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"

Client host	C. port	Server host	S. port	Start time
192.168.220.147 [win7pro32vm] (Windows)	49167	118.1.103.182	445	23/05/2017 11:27:16
192.168.220.147 [win7pro32vm] (Windows)	49168	192.168.220.1	445	23/05/2017 11:27:16
192.168.220.147 [win7pro32vm] (Windows)	49169	192.168.220.2	445	23/05/2017 11:27:08
192.168.220.147 [win7pro32vm] (Windows)	49180	68.120.94.85	445	23/05/2017 11:27:17
192.168.220.147 [win7pro32vm] (Windows)	49191	205.253.150.181	445	23/05/2017 11:27:18
192.168.220.147 [win7pro32vm] (Windows)	49195	177.176.218.128	445	23/05/2017 11:27:18
192.168.220.147 [win7pro32vm] (Windows)	49205	102.63.202.230	445	23/05/2017 11:27:19
192.168.220.147 [win7pro32vm] (Windows)	49208	168.33.235.108	445	23/05/2017 11:27:19
192.168.220.147 [win7pro32vm] (Windows)	49217	213.102.45.241	445	23/05/2017 11:27:20
192.168.220.147 [win7pro32vm] (Windows)	49219	111.41.94.9	445	23/05/2017 11:27:20
192.168.220.147 [win7pro32vm] (Windows)	49224	145.174.108.206	445	23/05/2017 11:27:21
192.168.220.147 [win7pro32vm] (Windows)	49231	15.125.80.112	445	23/05/2017 11:27:21
192.168.220.147 [win7pro32vm] (Windows)	49235	202.160.176.231	445	23/05/2017 11:27:22
192.168.220.147 [win7pro32vm] (Windows)	49238	158.126.229.230	445	23/05/2017 11:27:22
192.168.220.147 [win7pro32vm] (Windows)	49238	158.126.229.230	445	23/05/2017 11:27:34
192.168.220.147 [win7pro32vm] (Windows)	49238	158.126.229.230	445	23/05/2017 11:27:34
192.168.220.147 [win7pro32vm] (Windows)	49244	147.166.235.55	445	23/05/2017 11:27:22
192.168.220.147 [win7pro32vm] (Windows)	49244	147.166.235.55	445	23/05/2017 11:27:34
192.168.220.147 [win7pro32vm] (Windows)	49244	147.166.235.55	445	23/05/2017 11:27:34
192.168.220.147 [win7pro32vm] (Windows)	49247	152.170.180.219	445	23/05/2017 11:27:22
192.168.220.147 [win7pro32vm] (Windows)	49247	152.170.180.219	445	23/05/2017 11:27:34
192.168.220.147 [win7pro32vm] (Windows)	49247	152.170.180.219	445	23/05/2017 11:27:34
192.168.220.147 [win7pro32vm] (Windows)	49252	58.246.210.67	445	23/05/2017 11:27:23
192.168.220.147 [win7pro32vm] (Windows)	49252	58.246.210.67	445	23/05/2017 11:27:35
192.168.220.147 [win7pro32vm] (Windows)	49252	58.246.210.67	445	23/05/2017 11:27:35
192.168.220.147 [win7pro32vm] (Windows)	49254	155.154.108.212	445	23/05/2017 11:27:23
192.168.220.147 [win7pro32vm] (Windows)	49254	155.154.108.212	445	23/05/2017 11:27:35
192.168.220.147 [win7pro32vm] (Windows)	49254	155.154.108.212	445	23/05/2017 11:27:35
192.168.220.147 [win7pro32vm] (Windows)	49259	126.189.245.239	445	23/05/2017 11:27:23
192.168.220.147 [win7pro32vm] (Windows)	49259	126.189.245.239	445	23/05/2017 11:27:35
192.168.220.147 [win7pro32vm] (Windows)	49259	126.189.245.239	445	23/05/2017 11:27:35
192.168.220.147 [win7pro32vm] (Windows)	49263	90.231.143.65	445	23/05/2017 11:27:24

IoC – YARA

Questa regola yara e' in grado di rilevare le versioni piu' diffuse di wannacry:

```
rule WannaCryRansomwareGeneric {
	strings:
		$s0 = {410044004D0049004E0024} /*sequenze di byte*/
		$s1 = "WannaDecryptor“ /*stringhe*/
		$s2 = "WANNACRY"
		$s3 = "Microsoft Enhanced RSA and AES Cryptographic"
		$s4 = "PKS"
		$s5 = "StartTask"
		$s6 = "wcry@123"
		$s7 = {2F6600002F72}
		$s8 = "unzip 0.15 Copyrigh"
		$s9 = "Global\\WINDOWS_TASKOSHT_MUTEX"
		$s10 = "Global\\WINDOWS_TASKCST_MUTEX"
		$s11 = {7461736B736368652E65786500000000005461736B537461727400000074 2E776E7279000069636163}
		$s12 = {6C73202E202F6772616E742045766572796F6E653A46202F54202F43202F5100617474726962202B68}
		$s13 = "WNcry@2ol7"
		$s14 = "wcry@123"
		$s15 = "Global\\MsWinZonesCacheCounterMutexA“
	condition:
		($s0 and $s1 and $s2 and $s3 or $s4 and $s5 and $s6 and $s7 or $s8 and $s9 and $s10 or $s11 and $s12 or
$s13 or $s14 or $s15) and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550
}
rule MS17010WanaCryworm {
	strings:
		$ms17010_str1="PC NETWORK PROGRAM 1.0"
		$ms17010_str2="LANMAN1.0"
		$ms17010_str3="Windows for Workgroups 3.1a"
		$ms17010_str4="__TREEID__PLACEHOLDER__"
		$ms17010_str5="__USERID__PLACEHOLDER__"
		$wannacry_payload_substr1 = "h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j"
		$wannacry_payload_substr2 = "h54WfF9cGigWFEx92bzmOd0UOaZlM"
		$wannacry_payload_substr3 = "tpGFEoLOU6+5I78Toh/nHs/RAP"
	condition:
		all of them and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 /*Header dei PE*/
}
```

Conclusioni

✗ L'attacco, una volta ancora dopo Stuxnet, DuQu e Regin, ci permette di avere un tangibile esempio dei rischi connessi con la raccolta e il collezionamento di vulnerabilità a fini "borderline" da parte di agenzie governative occidentali.

✗ Questa è una importante fase per Internet… si discute di censura, sicurezza, nuove regole…

✗ Io sono dell'opinione che si dovrebbe iniziare a riflettere anche su questi casi e sul ruolo che ogni organizzazione governativa preposta alla cybersecurity deve svolgere e contemporaneamente alle responsabilità connesse con questo ruolo.

Una proposta che merita un dibattito

- Lo scorso Febbraio, da più parti, si è sollevata la proposta di creare una sorta di "Convenzione di Ginevra" sul cyberspazio.
- La proposta tende a favorire la voluntary disclosure di vulnerabilità identificate da agenzie governative al fine di migliorare il livello della Sicurezza generale (mondiale) e di mettere al bando ogni possibile utilizzo di queste vulnerabilità a fini di spionaggio economico e militare.
- Questa proposta, di fatto mai raccolta da rappresentanti governativi, è decisamente pregevole e merita di essere dibattuta in modo approfondito sia per quello che riguarda le sue conseguenze positive, sia per quello che concerne