smau R2B RESEARCH TO BUSINESS

BOLOGNA 7-8 GIUGNO 2018

Bologna Fiere

7 giugno ore 11:00
Arena SMAU ICT

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…

Relatori: Enrico Tonello – Federico Girotto


R.it
Sicurezza
Home
News
Speciali
Mobile
Social Network
Sicurezza
"WannaCry e le aziende? La disattenzione alla sicurezza è paradossale"
Intervista a Carlo Mauceli, CTO e
analizza i motivi del grande attacc
informazione e occorre maggio
Attacco hacker, cosa fare (e non fare) per difendersi da Wannacry
Carola Frediani
COMMENTI
«Ransomware» globale, nel giorno degli hacker colpiti anche ospedali inglesi
MONDO
CYBERSECURITY
Martedì 16 maggio 2017 - 15:50
Ministero difesa Russia: respinti tutti i cyberattacchi WannaCry
"immediatamente identificati e bloccati rapidamente"
IL SECOLO XIX
agi.it
Microsoft
Wannacry: "Già in 200 hanno pagato il riscatto"
NHS
CRONACA
"Un attacco senza precedenti". Chi è stato colpito da Wannacry

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Ransomware: cosa sono ?

Con il termine **Ransomware** definiamo tutti quei programmi o software che bloccano l'accesso ai file di documenti o al computer chiedendo un riscatto in denaro per accedervi.

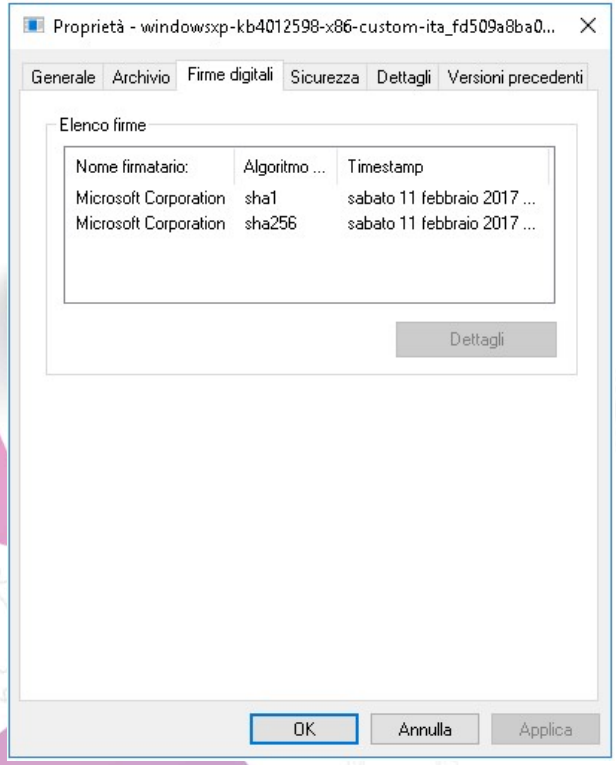
Con il termine **Crypto-Malware** definiamo un **ransomware** che va a **cifrare** i file di documenti o dati attraverso una password (chiave), rendendo impossibile l'accesso fino al pagamento di un riscatto in denaro.

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

WannaCry

- Prima apparizione ad aprile 2017
- Venerdì 12 maggio 2017 ➔ WannaCry 2.0
- Vettore di infezione: vulnerabilità di Windows ➔ **EternalBlue**
- Agosto 2016: Shadows Brokers vs Equation Group (NSA)
- Marzo 2017: Microsoft Patch MS17-010 per EternalBlue
- 14 Aprile 2017: Shadow Brokers rilascia pubblicamente il codice di EternalBlue

Microsoft Patch

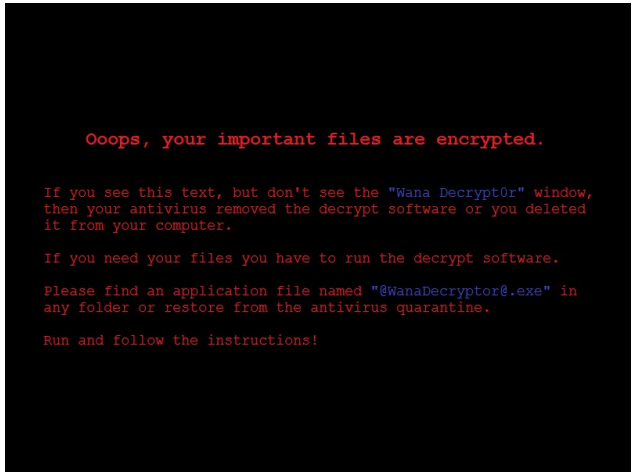


- Marzo 2017 Microsoft Patch MS17-010 per EternalBlue per tutti i sistemi operativi supportati
- 13 maggio 2017 Microsoft rilascia aggiornamento manuale per Windows XP – Server 2003 – Vista - Windows 8 – Server 2008: http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

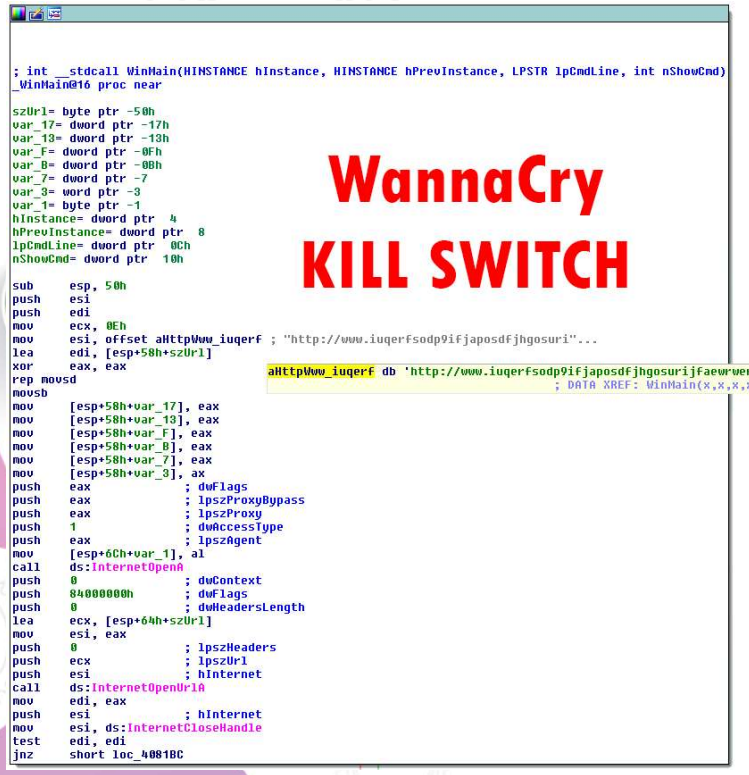
WannaCry

- Algoritmo di cifratura RSA
- Estensioni: .WCRY, .WNCRY
- Riscatto 300$ / 600$



Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

WannaCry KILL SWITCH



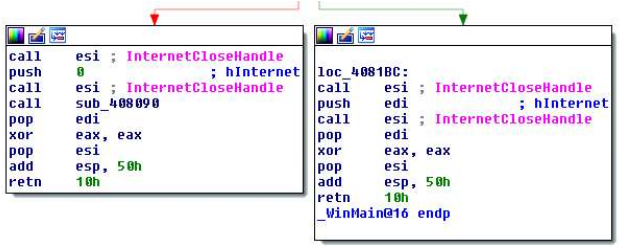

```
; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
_WinMain@16 proc near

szUrl= byte ptr -50h
var_17= dword ptr -17h
var_13= dword ptr -13h
var_F= dword ptr -0Fh
var_B= dword ptr -0Bh
var_7= dword ptr -7
var_3= word ptr -3
var_1= byte ptr -1
hInstance= dword ptr  4
hPrevInstance= dword ptr  8
lpCmdLine= dword ptr  0Ch
nShowCmd= dword ptr  10h

sub     esp, 50h
push    esi
push    edi
mov     ecx, 0Eh
mov     esi, offset aHttpWww_iuqerf ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
lea     edi, [esp+58h+szUrl]
xor     eax, eax
rep movsd
movsb
mov     [esp+58h+var_17], eax
mov     [esp+58h+var_13], eax
mov     [esp+58h+var_F], eax
mov     [esp+58h+var_B], eax
mov     [esp+58h+var_7], eax
mov     [esp+58h+var_3], ax
push    eax             ; dwFlags
push    eax             ; lpszProxyBypass
push    eax             ; lpszProxy
push    1               ; dwAccessType
push    eax             ; lpszAgent
mov     [esp+6Ch+var_1], al
call    ds:InternetOpenA
push    0               ; dwContext
push    84000000h       ; dwFlags
push    0               ; dwHeadersLength
lea     ecx, [esp+64h+szUrl]
mov     esi, eax
push    0               ; lpszHeaders
push    ecx             ; lpszUrl
push    esi             ; hInternet
call    ds:InternetOpenUrlA
mov     edi, eax
push    esi             ; hInternet
mov     esi, ds:InternetCloseHandle
test    edi, edi
jnz     short loc_4081BC

aHttpWww_iuqerf db 'http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com',0
                                        ; DATA XREF: WinMain(x,x,x,x)+A7o
```

- Kill Switch scoperto dal ricercatore MalwareTech (@MalwareTechBlog)



```
call    esi ; InternetCloseHandle
push    0               ; hInternet
call    esi ; InternetCloseHandle
call    sub_408090
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn    10h
```

```
loc_4081BC:
call    esi ; InternetCloseHandle
push    edi             ; hInternet
call    esi ; InternetCloseHandle
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn    10h
_WinMain@16 endp
```

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Quanto ha incassato WannaCry?

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Total Received: 14.08097351
Total Sent: 0.00000000
Final Balance: 14.08097351
Total transactions: 108

Recent transactions:

	Date ▼	Amount	Balance
●	2017-05-26 16:27:55	0.24660900	14.08097351
●	2017-05-25 12:59:55	0.01252403	13.83436451
●	2017-05-25 12:52:55	0.00834935	13.82184048
●	2017-05-25 12:52:41	0.00834935	13.81349113
●	2017-05-25 12:37:03	0.00626202	13.80514178
●	2017-05-25 12:34:31	0.00417468	13.79887976
●	2017-05-25 12:34:23	0.00417468	13.79470508
●	2017-05-25 12:32:34	0.00208734	13.79053040
●	2017-05-25 12:32:23	0.00208734	13.78844306
●	2017-05-25 12:32:13	0.00208734	13.78635572
●	2017-05-25 12:26:32	0.04174677	13.78426838
●	2017-05-24 12:19:03	0.00000737	13.74252161
●	2017-05-23 17:40:23	0.14019899	13.74251424
●	2017-05-23 07:57:01	0.00005525	13.60231525
●	2017-05-21 03:26:33	0.15000000	13.60226000
●	2017-05-21 03:16:44	0.00001000	13.45226000
●	2017-05-20 12:49:33	0.30627600	13.45225000
●	2017-05-20 09:31:19	0.14980000	13.14597400
●	2017-05-19 15:21:24	0.30799999	12.99617400
●	2017-05-19 14:31:18	0.00000734	12.68817401
●	2017-05-19 09:48:05	0.33679000	12.68816667
●	2017-05-19 06:34:33	0.00100000	12.35137667

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Total Received: 17.14531693
Total Sent: 0.00000000
Final Balance: 17.14531693
Total transactions: 105

Recent transactions:

	Date ▼	Amount	Balance
●	2017-05-29 09:06:39	0.13643100	17.14531693
●	2017-05-23 12:50:16	0.14000099	17.00888593
●	2017-05-22 20:27:25	0.00049776	16.86888494
●	2017-05-19 09:16:06	0.16101831	16.86838718
●	2017-05-19 04:45:15	0.31614227	16.70736887
●	2017-05-19 03:49:32	0.00010000	16.39122660
●	2017-05-18 20:09:19	0.34000000	16.39112660
●	2017-05-18 15:34:13	0.01322067	16.05112660
●	2017-05-18 04:59:35	0.00006000	16.03790593
●	2017-05-18 03:35:13	0.00493532	16.03784593
●	2017-05-17 10:01:19	0.16742500	16.03291061
●	2017-05-17 08:18:31	0.37620000	15.86548561
●	2017-05-17 04:48:49	0.33344400	15.48928561
●	2017-05-17 04:30:37	0.00290000	15.15584161
●	2017-05-17 00:35:15	0.17204597	15.15294161
●	2017-05-16 23:35:04	0.00013370	14.98089564
●	2017-05-16 23:34:25	0.00013370	14.98076194
●	2017-05-16 21:15:21	0.34500000	14.98062824
●	2017-05-16 19:15:51	0.17075120	14.63562824
●	2017-05-16 17:39:58	0.34171679	14.46487704
●	2017-05-16 15:28:35	0.17301900	14.12316025
●	2017-05-16 13:33:14	0.16991694	13.95014125

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Total Received: 19.54792267
Total Sent: 0.00000000
Final Balance: 19.54792267
Total transactions: 124

Recent transactions:

	Date ▼	Amount	Balance
●	2017-06-02 11:43:27	0.11947184	19.54792267
●	2017-05-26 16:21:12	0.13000000	19.42845083
●	2017-05-25 09:59:32	0.27000000	19.29845083
●	2017-05-25 05:34:02	0.00455900	19.02845083
●	2017-05-23 07:13:30	0.26800000	19.02389183
●	2017-05-23 06:16:00	0.00100000	18.75589183
●	2017-05-22 22:58:38	0.18990000	18.75489183
●	2017-05-19 12:50:15	0.02120000	18.56499183
●	2017-05-19 11:45:19	0.30770000	18.54379183
●	2017-05-18 22:32:16	0.00486966	18.23609183
●	2017-05-18 13:47:54	0.30996780	18.23122217
●	2017-05-18 09:55:07	0.33612000	17.92125437
●	2017-05-18 05:50:20	0.12250000	17.58513437
●	2017-05-17 22:42:29	0.33800400	17.46263437
●	2017-05-17 19:04:37	0.32551954	17.12463037
●	2017-05-17 12:06:18	0.19900000	16.79911083
●	2017-05-17 05:56:44	0.00001800	16.60011083
●	2017-05-17 05:37:13	0.16913661	16.60009283
●	2017-05-17 02:08:24	0.16982000	16.43095622
●	2017-05-16 23:35:04	0.00013370	16.26113622
●	2017-05-16 23:34:25	0.00013370	16.26100252
●	2017-05-16 23:01:33	0.11930000	16.26086882

```
00 F400: 6E 00 74 00  65 00 6C 00  00 00 00 00  25 00 73 00 n.t.e.l.....%.s.
00 F410: 5C 00 50 00  72 00 6F 00  67 00 72 00  61 00 6D 00 \.P.r.o.g.r.a.m.
00 F420: 44 00 61 00  74 00 61 00  00 00 00 00  63 6D 64 2E D.a.t.a.....cmd.
00 F430: 65 78 65 20  2F 63 20 22  25 73 22 00  58 49 41 00 exe /c "%s".XIA.
00 F440: 31 31 35 70  37 55 4D 4D  6E 67 6F 6A  31 70 4D 76 115p7UMMngoj1pMv
00 F450: 6B 70 48 69  6A 63 52 64  66 4A 4E 58  6A 36 4C 72 kpHijcRdfJNXj6Lr
00 F460: 4C 6E 00 00  31 32 74 39  59 44 50 67  77 75 65 5A Ln..12t9YDPgwueZ
00 F470: 39 4E 79 4D  67 77 35 31  39 70 37 41  41 38 69 73 9NyMgw519p7AA8is
00 F480: 6A 72 36 53  4D 77 00 00  31 33 41 4D  34 56 57 32 jr6SMw..13AM4VW2
00 F490: 64 68 78 59  67 58 65 51  65 70 6F 48  6B 48 53 51 dhxYgXeQepoHkHSQ
00 F4A0: 75 79 36 4E  67 61 45 62  39 34 00 00  25 73 25 64 uy6NgaEb94..%s%d
00 F4B0: 00 00 00 00  47 6C 6F 62  61 6C 5C 4D  73 57 69 6E ....Global\MsWin
00 F4C0: 5A 6F 6E 65  73 43 61 63  68 65 43 6F  75 6E 74 65 ZonesCacheCounte
00 F4D0: 72 4D 75 74  65 78 41 00  74 61 73 6B  73 63 68 65 rMutexA.tasksche
00 F4E0: 2E 65 78 65  00 00 00 00  54 61 73 6B  53 74 61 72 .exe....TaskStar
00 F4F0: 74 00 00 00  74 2E 77 6E  72 79 00 00  69 63 61 63 t...t.wnry..icac
00 F500: 6C 73 20 2E  20 2F 67 72  61 6E 74 20  45 76 65 72 ls . /grant Ever
00 F510: 79 6F 6E 65  3A 46 20 2F  54 20 2F 43  20 2F 51 00 yone:F /T /C /Q.
00 F520: 61 74 74 72  69 62 20 2B  68 20 2E 00  57 4E 63 72 attrib +h ..WNcr
00 F530: 79 40 32 6F  6C 37 00 00  2F 69 00 00  01 00 00 00 y@2ol7../i.....
00 F540: 08 00 00 00  02 00 00 00  04 00 00 00  10 00 00 00 ................
00 F550: 80 00 00 00  20 00 00 00  40 00 00 00  47 65 74 4E ....  ...@...GetN
00 F560: 61 74 69 76  65 53 79 73  74 65 6D 49  6E 66 6F 00 ativeSystemInfo.
```

Al 5 giugno 2017 ➔ 50,77 BTC

Al 5 giugno 2018 ➔ 53,94 BTC

1 BTC in USD = 7.724,07

quotazione al 5 giugno 2018

Totale in USD: **400.423,23 $**

Transazioni totali al 05/06/2018

Entrate 382 – Uscite 6 = 376

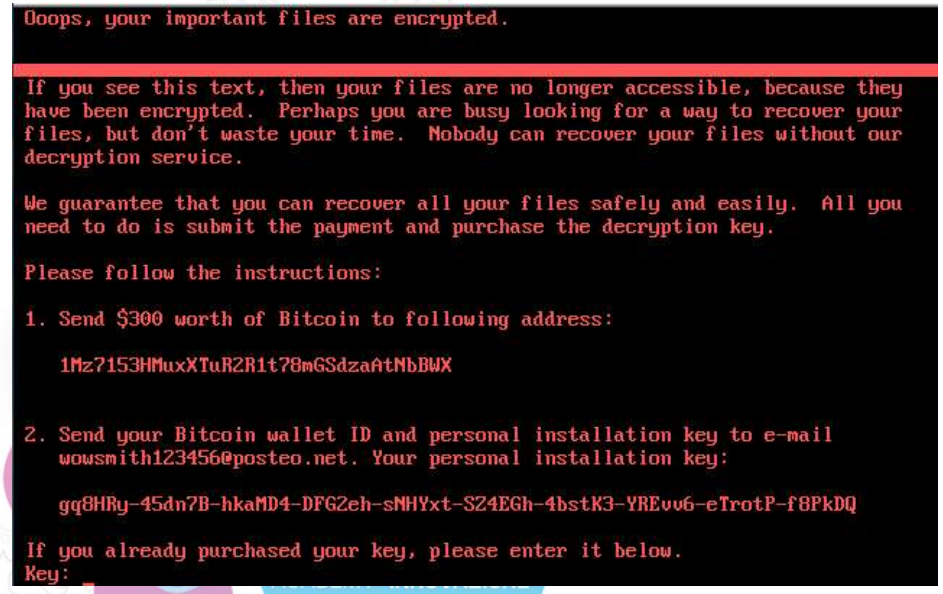
Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

NotPetya / EternalPetya

- Martedì 27 giugno 2017 ➔ NotPetya / EternalPetya
- Vettore di infezione 1: M.E. Doc server (ZvitPublishedObjects.dll). Attacco al Server di distribuzione software M.E. Doc con modifica di una .dll. Tutti gli aggiornamenti successivi degli utilizzatori di questo software sono diventati diffusori del Ransomware
- Vettore di infezione 2: vulnerabilità di Windows ➔ **EternalBlue**
- Vettore di infezione 3: utilizza le tecniche WMIC – PsExec (utility SysInternal). Esecuzione software da remoto
- Gruppo (sospettato): Telebots (Xdata Ransomware)

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

NotPetya / EternalPetya



- Si basa su Petya 4.0 GoldenEye, ma non è una nuova variante di Petya
- Algoritmo di cifratura: AES (file) + Salsa20 (MFT)
- Estensioni: nessuna estensione per i file
- Riscatto: 300$ in Bitcoin
- Anomalie: i file cifrati possono essere recuperati pagando il riscatto, ma la MFT è cifrata con una chiave casuale non collegata al'ID della vittima che non permette il recupero anche pagando il riscatto
- Ransomware o wiper ?

NotPetya / EternalPetya vs Petya 4.0

- Il cuore del codice di **Petya** è memorizzato dal settore 1 al 15 (0xf). Mettendo a confronto queste 2 aree tra **EternalPetya** e **GoldenEye Petya differiscono solamente per 43 byte**

NotPetya/Eternal Petya

```
seg000:847D                 pop     bx
seg000:847E                 lea     ax, [bp+var_1A3]
seg000:8482                 push    ax
seg000:8483                 call    sub_88C4
seg000:8486                 pop     bx
seg000:8487                 push    9F6Ch
seg000:848A                 call    sub_85DE
seg000:848D                 pop     bx
seg000:848E                 nop
seg000:848F                 nop
seg000:8490                 nop
seg000:8491                 push    9F71h
seg000:8494                 call    sub_85DE
seg000:8497                 pop     bx
seg000:8498                 mov     si, [bp+arg_0]
seg000:849B
seg000:849B loc_849B:                               ; CODE XREF: sub_8426+BB↓j
seg000:849B                 push    9FAEh
seg000:849E                 call    sub_85DE
seg000:84A1                 pop     bx
seg000:96D4                 enter   16h, 0
seg000:96D8                 push    di
seg000:96D9                 push    si
seg000:96DA                 mov     byte ptr [bp+var_12+1], 31h ; '1'
seg000:96DE                 mov     [bp+var_10], 6Eh ; 'n'
seg000:96E2                 mov     [bp+var_F], 76h ; 'v'
seg000:96E6                 mov     [bp+var_E], 61h ; 'a'
seg000:96EA                 mov     [bp+var_D], 6Ch ; 'l'
seg000:96EE                 mov     [bp+var_B], 64h ; 'd'
seg000:96F2                 mov     [bp+var_A], 20h ; ' '
seg000:96F6                 mov     [bp+var_9], 73h ; 's'
seg000:96FA                 mov     [bp+var_8], 33h ; '3'
seg000:96FE                 mov     [bp+var_7], 63h ; 'c'
seg000:9702                 mov     [bp+var_6], 74h ; 't'
seg000:9706                 mov     al, 2Dh ; '-'
seg000:9708                 mov     byte ptr [bp+var_12], al
seg000:970B                 mov     [bp+var_5], al
seg000:970E                 mov     al, 69h ; 'i'
seg000:9710                 mov     [bp+var_C], al
seg000:9713                 mov     [bp+var_4], al
```

Petya GoldenEye 4.0

```
seg000:847D                 pop     bx
seg000:847E                 lea     ax, [bp+var_1A3]
seg000:8482                 push    ax
seg000:8483                 call    sub_88C4
seg000:8486                 pop     bx
seg000:8487                 push    9F16h
seg000:848A                 call    sub_85DE
seg000:848D                 pop     bx
seg000:848E                 call    sub_896A
seg000:8491                 push    9F1Ch
seg000:8494                 call    sub_85DE
seg000:8497                 pop     bx
seg000:8498                 mov     si, [bp+arg_0]
seg000:849B
seg000:849B loc_849B:                               ; CODE XREF: sub_8426+BB↓j
seg000:849B                 push    9F5Ch
seg000:849E                 call    sub_85DE
seg000:84A1                 pop     bx
seg000:84A2                 mov     byte ptr [bp+var_1], 0
seg000:84A6
seg000:96D4                 enter   16h, 0
seg000:96D8                 push    di
seg000:96D9                 push    si
seg000:96DA                 mov     byte ptr [bp+var_12+1], 78h ; 'x'
seg000:96DE                 mov     [bp+var_10], 70h ; 'p'
seg000:96E2                 mov     [bp+var_F], 61h ; 'a'
seg000:96E6                 mov     [bp+var_E], 6Eh ; 'n'
seg000:96EA                 mov     [bp+var_D], 64h ; 'd'
seg000:96EE                 mov     [bp+var_B], 33h ; '3'
seg000:96F2                 mov     [bp+var_A], 32h ; '2'
seg000:96F6                 mov     [bp+var_9], 2Dh ; '-'
seg000:96FA                 mov     [bp+var_8], 62h ; 'b'
seg000:96FE                 mov     [bp+var_7], 79h ; 'y'
seg000:9702                 mov     [bp+var_6], 74h ; 't'
seg000:9706                 mov     al, 65h ; 'e'
seg000:9708                 mov     byte ptr [bp+var_12], al
seg000:970B                 mov     [bp+var_5], al
seg000:970E                 mov     al, 20h ; ' '
seg000:9710                 mov     [bp+var_C], al
seg000:9713                 mov     [bp+var_4], al
```


Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

NotPetya / EternalPetya

Alexander Adamov
@Alex_Ad
Following

#EternalPetya ransomware analysis
nioguard.blogspot.com/2017/06/eterna …
#Petya #Ransomware #Nioguard

Traduci dalla lingua originale: danese

18:05 - 28 giu 2017 da Ucraina

Tweet fissato

JANUS @JanusSecretary · 5 lug
"They're right in front of you and can open very large doors" mega.nz /#!lmow0Z7D!lny… @hasherezade @MalwareTechBlog ;)

Traduci dalla lingua originale: inglese

2 58 66

JANUS @JanusSecretary · 28 giu
we're back havin a look in "notpetya" maybe it's crackable with our privkey #petya @hasherezade sadly missed ;)

Traduci dalla lingua originale: inglese

14 60 74

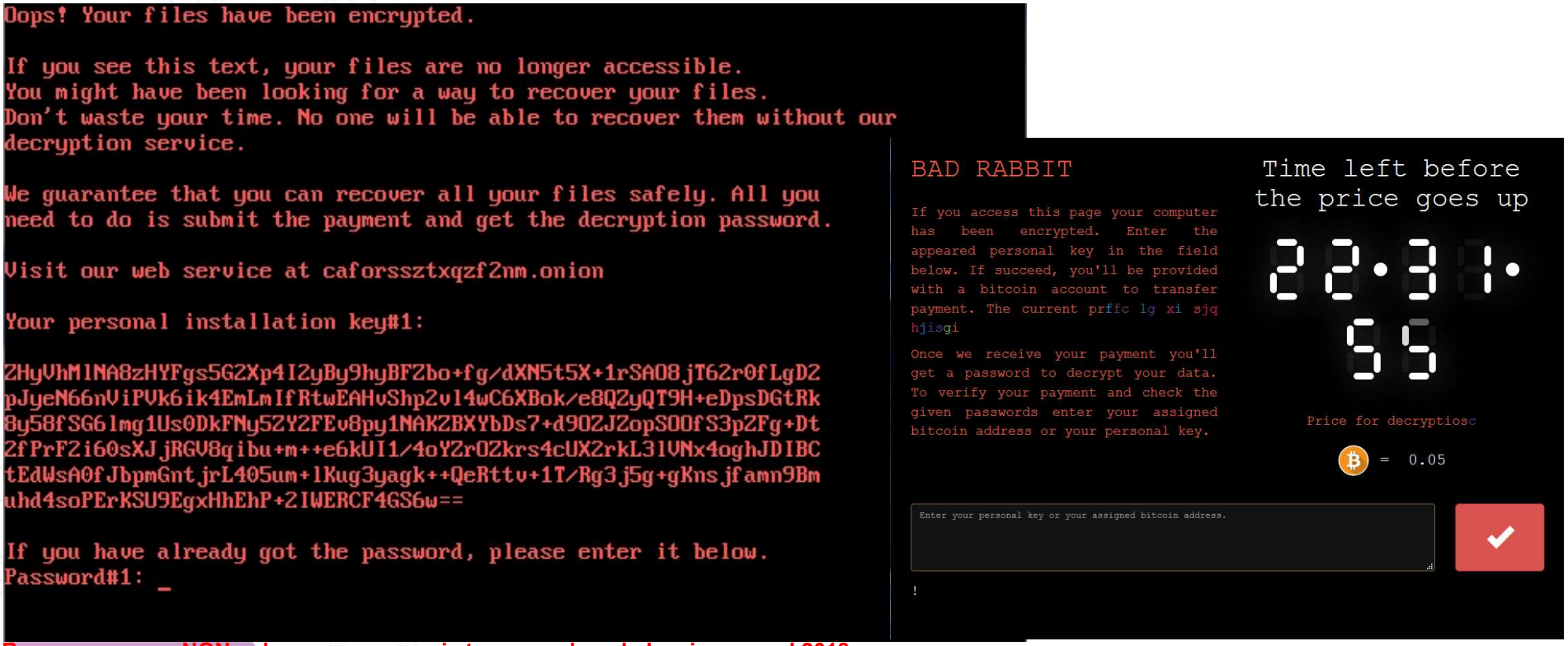
Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

Bad Rabbit

- Martedì 24 ottobre 2017 ➔ Bad Rabbit
- Vettore di infezione 1: Siti compromessi (finto flash player)
- Vettore di infezione 2: Samba con attacco brute force delle credenziali. Spostamento laterale.
- Cifra: file + disco (usa il driver di DiskCryptor per cifrare il disco). Cifratura con software OpenSource.

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Bad Rabbit



Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto


Italiano
Português
Español
Français
Nederlands
Istruzioni per il recupero dei file
Probabilmente hai notato che non puoi più aprire i tuoi file e alcuni software hanno smesso di funzionare correttamente.
Questo era previsto. I tuoi file si trovano ancora al loro posto, ma sono stati crittografati da "SAGE 2.0 Ransomware".
I tuoi file non sono persi, è possibile farli tornare al loro stato normale eseguendo una decrittazione.
L'unico modo in cui è possibile farlo è scaricare il software "SAGE Decrypter"
Your files has been safely encrypted
Decryptionkey
SERPENT RANSOMWARE
Home
FAQ
Instructions
Support
Temporary offer! Click here to decrypt 2 files for FREE!
Your documents, photos, videos, databases and other important files have been encrypted!
To restore your files you can buy special software 'Serpent Decrypter'
If you pay within 7 days the price is 0.50 bitcoins (~€525)
After 7 days the price will rise to 1.5 bitcoins (~€1575)
The special price will end in
8d 23h 36m 3s
GLOBE
Your files are Encrypted!
Your personal ID
Your documents, photos, databases, and
For data recovery
To buy the decryptor, you
on the Bitcoin wallet:
(Buy Bitcoins can be here https://localbitcoins.com/buy_bitcoi
After the payment, send a letter
In the letter inch
response lette
start decryp
COMODO
YOUR FILES ARE ENCRYPTED!
06 days 08:59:33 0742
Your files are encrypted!
Your personal ID
All your important data has been encrypted.
To recover data you need decryptor.
To get the decryptor
pay for decrypt:
site for buy bitcoin:
Buy 1 BTC on one of these sites
1. https://localbitcoins.com
2. https://www.coinbase.com
3. https://xchange.cc
bitcoin adress for pay:
Send 1 BTC for decrypt
fter the payment:
you will

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Ransomware Time Line 2017

2017-01
Renamer
CryptoShield
Merry X-mas
Spora
Sage
Globe

2017-02
CryptoFAG
GpCode
UnLock26

2017-03
Revenge

2017-04
WannaCry 1.0
CryptoWIRE
DoNotChange
LambdaLocked
Matrix
CryptoTrump
Serpent
CryptoNM4

2017-05
Hermes 2.0
GlobeImp2
CryptoXDATA
CryptoMole
CryptoPEC
CryptoMay
WannaCry 2.0

2017-06
NotPetya
EternalPetya

2017-07
GPAA
Spectre

2017-08
SyncCrypt

2017-09
NudeRansom
RedBoot
InfinityLock
PayOrDie
HappyCrypter
Paradise
SyncAck

2017-10
Bad Rabbit
Magniber
New Anubi

2017-11
CryptoScarab

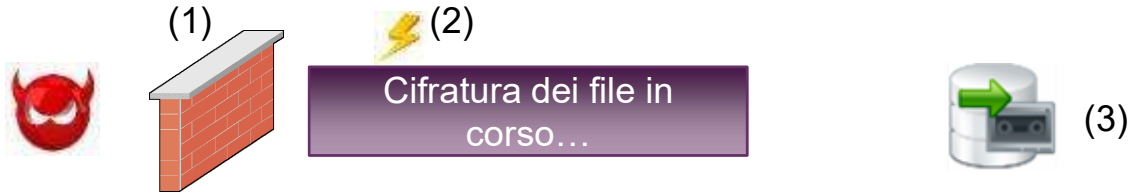
2017-12

2017

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Come difendersi dai Ransomware



Protezione multi-livello per difendersi dai ransomware:

- Anti-virus attivo e sempre aggiornato!
- Windows, ma anche Java, Adobe Reader, Adobe Flash Player sempre aggiornati!
- Password degli utenti e dell'administrator complesse e non banali!
- **Protezione anti-ransomware ➔ mitigazione dell'attacco**
- Backup!!!

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Come difendersi dai Ransomware

Simulazione su VM di come la protezione VirIT Anti-Ransomware mitiga l'attacco dei seguenti ransomware:

- WannaCry

TG Soft
Security Software Specialist
ANTIVIRUS · ANTISPYWARE · ANTIMALWARE
www.tgsoft.it

VirIT explorer PRO
L'AntiVirus, AntiSpyware, AntiMalware ITALIANO

C.R.A.M. CENTRO RICERCHE ANTI-MALWARE

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Ransomware in Italia 2018

- Gli attacchi Ransomware generalizzati sembrerebbero essersi «acquietati»… forse la quiete prima della tempesta… ?
- Persistono gli attacchi ai Server da parte di **Dharma** e sue varianti che effettuano attacco Brute-Force all'RDP (Desktop remoto) – Attacco MitM (Man in the Middle).
- Nei primi 4 mesi del 2018 gli attacchi maggiormente significativi arrivano da GandCrab 1.0, 2.0 e 3.0 (2018)
- Principali caratteristiche di GandCrab e le sue varianti:
  - Algoritmo di cifratura: RSA (file)
  - Estensioni: .CRAB; .GDCB
  - Riscatto: 400$ - 1200$ in Bitcoin / DASH dopo 48h il riscatto richiesto raddoppia.

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto

I creatori di Malware cosa stanno facendo

- I creatori di Malware non si sono certo redenti (… forse qualcuno sì…), ma si sono dedicati ad attività meno impattive, forse anche più remunerative, ma soprattutto, più silenti:
  - La creazione e diffusione di Malware per l'estrazione di CryptoValute (Mining) sfruttando le risorse di calcolo dei computer infettati;
  - La creazione di Malware atti all'esfiltrazione di dati (spyware, banker, pswstealer) con particolare attenzione alle password dell'Home Banking, dei Social Network, degli account e-mail etc. etc.;

Malware per «minare» Crypto Valute 1/2

- Modalità principali di diffusione:
  - Attraverso **campagne di Malspam** che cercano di indurre l'utente a scaricare il file in allegato o cliccare sul link da dove questo si attiva infettando la macchina, generalmente attraverso Dropper offuscati o altre tecniche in grado di sfuggire anche alle SandBox;
  - Attraverso la **compromissione di pagine WEB** ufficiali con inoculazione di codici di Mining in grado anche di scaricare e attivare Malware di Mining, così da estratte Crypto Valute anche dopo la chiusura della pagina WEB compromessa;
  - A volte **anche pagine WEB ufficiali** di servizi gratuiti (ad es. WEB radio o altro) integrano volutamente codici di Mining per minare a loro volta, in modo più o meno lecito, CryptoValute sfruttando le risorse di calcolo degli utenti.

Malware per «minare» Crypto Valute 2/2

- Obiettivo: Guadagnare sfruttando le potenzialità di calcolo degli ignari utenti;
- Contrariamente ai Ransomware i codici di Mining non producono impatti devastanti sui computer degli utenti ma certamente producono un deterioramento delle prestazioni nell'uso quotidiano;
- Cosa rubano allora:
  - Potenza di calcolo alle nostre CPU;
  - La nostra corrente elettrica;
  - Indirettamente rubano il nostro denaro!!!

Malware per l'esfiltrazione di dati - Spyware

- **Spyware**: Malware specificatamente progettati per esfiltrare dati e, attraverso funzionalità di keylogging, anche Login e Password dell'Home Banking, dei Social Network, degli account e-mail etc. etc.;

- Principali campagne Malspam, molto attive anche in Italia, atte alla diffusione di vari Spyware-Keylogger. :
  - AdWind;
  - UrSnif;
  - Zeus / Panda;
  - GootKit;
  - NanoCore.

  Acquistabili in abbonamento anche nel DarkWeb (SaaS = Software as a Service).

Campagne Malspam UrSnif

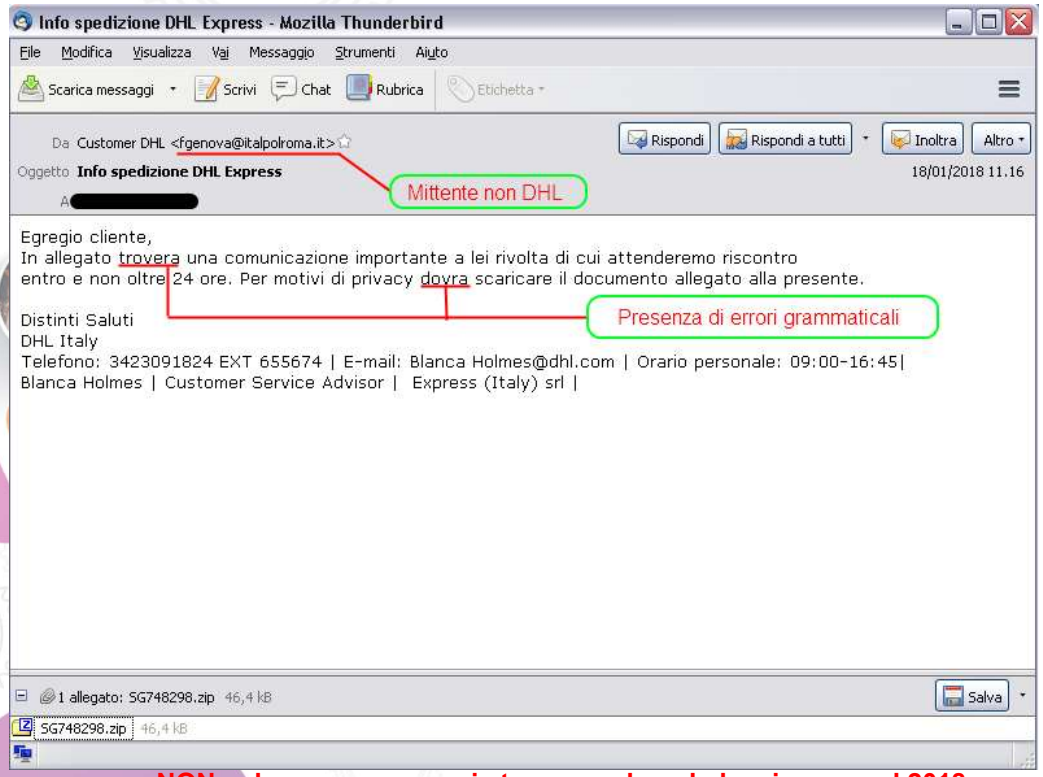
- **Le principali campagne di Malspam che diffondono UrSnif:**
  - Campagna DHL
  - Campagna «*Vedi Allegato e di confermare*»

Si tratta di un approccio di ingegneria sociale (Social Engineering), non nuovo, ma sempre e comunque efficace.

La **campagna DHL** è una mail che invita ad aprire l'allegato che contiene informazioni su un'ipotetica consegna per il tramite del vettore omonimo.

La campagna «***Vedi Allegato e di confermare***» è di una semplicità disarmante poiché induce in modo semplice ed efficacissimo il malcapitato ricevente ad aprire l'allegato poiché gli viene richiesto di confermare (non si sa cosa…) e questo solletica la curiosità… Mail di risposta che giunge da persona conosciuta!!!

UrSnif – Campagna DHL



- Mittente con Alias simil DHL ma con mail mittente NON coerente.
- Mail che si spacciano per DHL ma con errori grammaticali.

UrSnif – Campagna «Vedi allegato…»

Campagna «Vedi Allegato e di confermare»

- **UrSnif è uno Spyware-Keylogger in grado di rubare le password dell'Home Banking, degli account e-mail, dei social Network e altro…**
  - Furto Login e Password Home Banking ➔ accesso ai Conti Bancari, tentativi di effettuare Bonifici…
  - Furto Login e Password account E-mail ➔ accesso all'account per l'invio di e-mail di malspam come risposta alle mail ricevute ➔ Incremento della BotNet di diffusione del malware…

UrSnif – Campagna «Vedi allegato…»

Re: [redacted] - Mozilla Thunderbird

File Modifica Visualizza Vai Messaggio Strumenti Aiuto

Da Marco [redacted] <[redacted]@[redacted]> Rispondi | Rispondi a tutti | Inoltra | Altro

Oggetto **Re:** [redacted] 05/04/2018 06:48

A info@[redacted]

Buongiorno,

Vedi allegato e di confermare.

Ciao
Marco

1 allegato: Richiesta.doc 163 kB Salva

Richiesta.doc 163 kB

- **Mittente CONOSCIUTO**
- **Mail ricevuta in risposta ad una mail inviata…**

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

Conclusioni 1/2

- Anche per il 2018, seppure in calo, i ransomware continuano ad essere una minaccia letale per i nostri dati.
- Dall'autunno 2017 si stanno diffondendo campagne di Malspam sempre più sofisticate i cui autori sono vere e proprie organizzazioni criminali, che lavorano a livello industriale, sfornando anche più volte al giorno nuove varianti. Si tratta di vere e proprie organizzazioni criminali.
- Continua l'utilizzo dell'ingegneria sociale (social engineering) per indurre il ricevente a cliccare sull'allegato, pratiche di cui abbiamo visto in già da anni l'utilizzo da parte di Ransomware o di Spyware-Keylogger, poiché sfruttano il punto più debole del binomio uomo-macchina… l'uomo! (Vedi Allegato e di confermare…)

Conclusioni 2/2

- **Vir.IT eXplorer PRO** permette di proteggere i propri dati da attacchi Ransomware mitigando la cifratura dei file salvando la vittima
- Il backup può essere una soluzione, ma non sempre viene eseguito oppure quando non viene cifrato può essere obsoleto. Tempo di ripristino!!!
- Protezione multi-layer: AV + Anti-Ransomware + Backup
- La **consapevolezza degli utenti** è ormai fondamentale per NON cadere nei tranelli dell'ingegneria sociale (social engineering) e non farsi rubare le credenziali di accesso ai nostri dati più preziosi.
- **Vir.IT eXplorer PRO** offre supporto tecnico per l'analisi preventiva di file o mail sospette.

Vir.IT explorer PRO
L'AntiVirus, AntiSpyware, AntiMalware ITALIANO

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

smau R2B RESEARCH TO BUSINESS

BOLOGNA 7-8 GIUGNO 2018

Bologna Fiere

??? DOMANDE ???

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…

Relatori: Enrico Tonello & Federico Girotto

smau R2B RESEARCH TO BUSINESS
BOLOGNA 7-8 GIUGNO 2018
Bologna Fiere

GRAZIE dell'ATTENZIONE

TG Soft
Security Software Specialist
ANTIVIRUS • ANTISPYWARE • ANTIMALWARE
www.tgsoft.it

ing. Enrico Tonello

(info@tgsoft.it)

Federico Girotto

(f.girotto@viritpro.com)

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

https://www.facebook.com/viritexplorer

Ransomware ma NON solo… ecco come si stanno evolvendo le minacce nel 2018…
Relatori: Enrico Tonello & Federico Girotto