CYBER THREAT INTELLIGENCE REPORT
BAD RABBIT RANSOMWARE

Roma, 30-10-2017 – **TLP: WHITE – RISK : HIGH**

Contents

Executive Summary 1
Descrizione dell'incidente / infezione 5
Indicatori di Compromissione (IoC) 21
Artefact associati al Ransomware 23
Lista dei siti web attualmente compromessi 25
Yara Rule Set 26
Credenziali incluse nel ransomware 29

Executive Summary

Admiralty Code

A1

Completely reliable/Confirmed by other sources

Ransomware **Target Type**	Raccolta di informazioni di sistema e di dati confidenziali, **Goal**	Sconosciuto **Threat Actor involved**
Settore Finanziario, Media, Infrastrutture crtiche **Target Industry**	Ucraina, Russia, Germania, Turchia, USA, Europa **Effected Countries**	Drive-by downloads **Campaign**
PDL e Server Aziendali **Target Asset**	Javascript, Adobe Flash, Exploit **Delivery and Exploitation**	24 -10-2017 **Last Detection Date**
Action on target • Eseguire il backup di dati importanti • Aggiornare i sistemi operativi e i sistemi di sicurezza • Isolare i PC infetti • Bloccare gli IP e i domain infetti		Interfax, Fontanka, Aeroporto di Odessa, metropolitana Kiev **Target Sources**

Dettagli della Minaccia

L'obiettivo del report è quello di fornire **le informazioni disponibili** alla data di redazione di questo report **(comprese le conseguenti raccomandazioni tecniche)** e relative all'infezione su larga scala derivanti dalla diffusione di un ransomware denominato ***Bad Rabbit*** che è stato appurato **basarsi sul codice No-Petya** diffusosi nel giugno del 2017.

La prima segnalazione dell'attacco è avvenuta intorno alle 12:00 GMT del 24.10.2017.

Sebbene sono state registrate decine di migliaia gli attacchi informatici legati a questa infezione, i principali target sono aziende principalmente localizzate in Ucraina, Russia, Bulgaria, Germania, Turchia e Giappone. In particolare sono state accertate compromissioni nelle seguenti infrastrutture:

- Fontanka.ru
- Interfax News

- Kiev Metro
- Ministry of Infrastructure of Ukraine
- Odessa International Airport

L'infezione del ransomware avviene attraverso un attacco di tipo "drive-by download" su un sito che ospita una **falsa versione di un aggiornamento del programma Adobe Flash**. Il codice (dropper) malevolo era contenuto nelle cartelle */index.php* e */flash_install.php* del sito utilizzato per la diffusione del programma infetto è hxxp://1dnscontrol[.]com.

Una volta che un dispositivo è stato infettato da Bad Rabbit, il ransomware cerca determinati tipi di file per cifrarli. Successivamente il ransomware cifra l'intero contenuto del disco e visualizzata una schermata relativa al riscatto quando il computer viene riavviato. La crittografia del disco e del *bootloader*, attraverso dall'utility denominata *DiskCryptor*, realizzata dal ransomware Bad Rabbit è probabilmente basata sull'algoritmo AES in CBC mode.

Quando un computer infetto si riavvia, gli utenti vengono informati che i loro file sono stati crittografati e sono invitati a effettuare un pagamento pari a 0.05 bitcoin per ottenere la password necessaria per la decifratura degli stessi. La stessa schermata, consente alle vittime che hanno già ricevuto una password per l'accesso e l'avvio del proprio sistema. Il sito di pagamento è il TOR *hidden service* hxxp://caforssztxqzf2nm[.]onion. I *wallet* utilizzati per il recupero del riscatto sono i seguenti:

- 1GxXGMoz7HAVwRDZd7ezkKipY4DHLUqzmM;
- 17GhezAiRhgB8DGArZXBkrZBFTGCC9SQ2Z.

L'analisi del dominio TOR ha rilevato che il sito è stato preparato sin dal 19 ottobre e il certificato digitale contenuto nel codice malevolo è stato sottoscritto il 25 ottobre (nonostante l'attacco è iniziato il 24 ottobre) , mentre la data del 22 ottobre si riferisce alla compilazione di alcuni parti del codice malevolo. Queste informazioni temporali sono indicative di una precisa pianificazione dell'inizio della campagna per il 25 ottobre.

FileVersionInfo properties	
Copyright	Copyright © 1996-2017 Adobe Systems Incorporated
Product	Adobe® Flash® Player Installer/Uninstaller
Original name	FlashUtil.exe
Internal name	Adobe® Flash® Player Installer/Uninstaller 27.0
File version	27,0,0,170
Description	Adobe® Flash® Player Installer/Uninstaller 27.0 r0
Signature verification	The digital signature of the object did not verify.
Signing date	6:30 PM 10/25/2017

PE header basic information	
Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2017-10-22 02:33:58
Entry Point	0x000012C0
Number of sections	5

Figure 1 - Certificato presente nel ransomware

L'infezione viene propagata attraverso i seguenti servizi

- SVCCTL: the remote service management
- SMB2
- SMB
- NTLMSSP authentication brute force
- WMI

Inoltre viene utilizzato anche l'exploit chiamato *EternalRomance*.

Bad Rabbit non sembra contenere alcuna funzionalità di *wiper,* il che fa pensare che l'obiettivo dell'infezione sia la riscossione di un riscatto e, quindi, i cyber criminali avrebbero potenzialmente la capacità di fornire la password per decifrare i file e consentire

al computer di avviare il sistema operativo. **Al momento, non ci sono evidenze che la password per la decifratura dei file sia stata fornita dopo il pagamento del riscatto**.

Di seguito viene descritto il flusso logico degli step operativi svolti da BadRabbit.

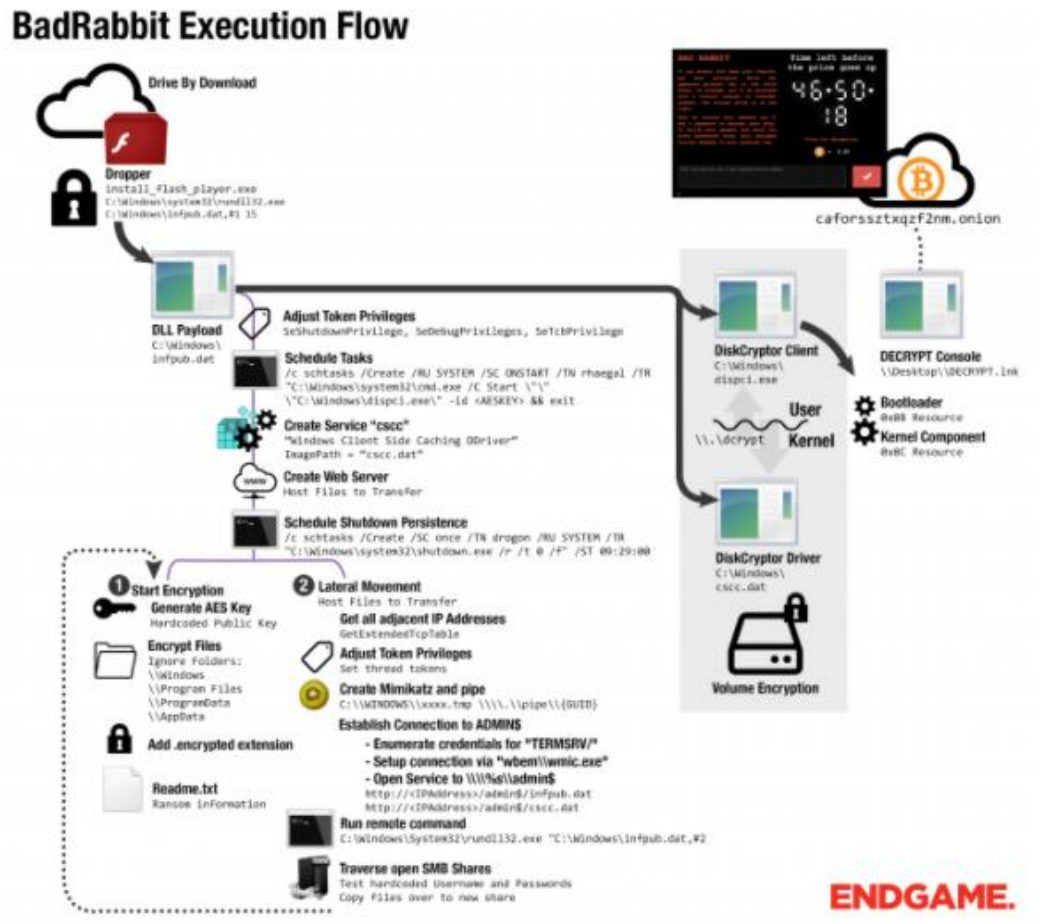

Figure 2 - Step operativi svolti da Bad Rabbit

La campagna in esame è attualmente in fase di monitoraggio. Per maggiori dettagli tecnici relativi all'infezione contattare il team specialistico tramite hunting@deepcyber.it *oppure info@deepcyber.it.*

Descrizione dell'incidente / infezione

L'attaccante (o il gruppo di attaccanti) dietro la campagna di diffusione del codice malevolo si sta diffondendo principalmente verso i seguenti target:

- transportation organizations
- governmental organizations
- media outlets

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).

DISTRIBUZIONE DEL DROPPER DEL RANSOMWARE

Uno dei metodi di distribuzione del ransomware Bad Rabbit avviene attraverso l'attacco *drive by download* da un sito compromesso. Per la prima compromissione si è iniettato un codice javascript (chiamato ***page-main.js*** e avente impronta hash 4f61e154230a64902ae035434690bf2b96b4e018) nel corpo del codice HTML della pagina *hxxp://185.149.120[.]3/scholargoogle* che attualmente non risulta più disponibile. La logica *Server side* dello script può determinare se il visitatore della pagina web può essere di interesse e, in questo caso, è mostrato un popup che chiede all'utente di scaricare un aggiornamento del programma Flash Player:

Drive-by downloads are a common method of spreading malware. Cybercriminals look for insecure web sites and plant a malicious script into HTTP or PHP code on one of the pages. This script may install malware directly onto the computer of someone who visits the site, or it may take the form on an IFRAME that re-directs the victim to a site controlled by the cybercriminals. In many cases the script is obfuscated, to make it more difficult for security researchers to analyse the code. Such attacks are called 'drive-by downloads' because they require no action on the part of the victim — beyond simply visiting the compromised web site: they are infected automatically (and silently) if their computer is vulnerable in some way (e.g. if they have failed to apply a security update to one of their applications).

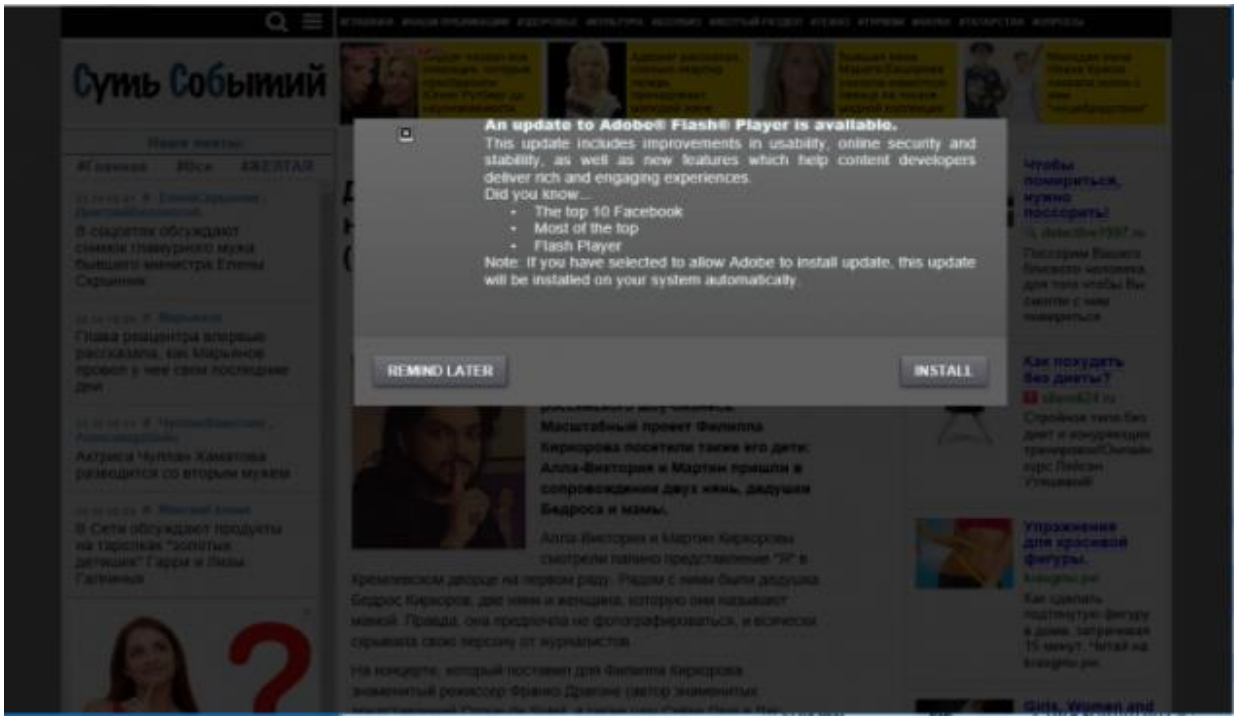

Figure 3 - Popup che invita l'utente a scaricare il dropper del ransomware

Altri siti che sono stati identificati come compromessi dal codice javascript sono i seguenti:

- hxxp://argumentiru[.]com
- hxxp://www.fontanka[.]ru
- hxxp://grupovo[.]bg
- hxxp://www.sinematurk[.]com
- hxxp://www.aica.co[.]jp
- hxxp://spbvoditel[.]ru
- hxxp://argumenti[.]ru
- hxxp://www.mediaport[.]ua
- hxxp://blog.fontanka[.]ru
- hxxp://an-crimea[.]ru
- hxxp://www.t.ks[.]ua
- hxxp://most-dnepr[.]info
- hxxp://osvitaportal.com[.]ua
- hxxp://www.otbrana[.]com

- hxxp://calendar.fontanka[.]ru
- hxxp://www.grupovo[.]bg
- hxxp://www.pensionhotel[.]cz
- hxxp://www.online812[.]ru
- hxxp://www.imer[.]ro
- hxxp://novayagazeta.spb[.]ru
- hxxp://i24.com[.]ua
- hxxp://bg.pensionhotel[.]com
- hxxp://ankerch-crimea[.]ru

ANALISI DEL DROPPER DEL RANSOMWARE

Quando un utente accetta di scaricare l'aggiornamento proposto su un website compromesso, viene avviato il download dell'eseguibile install_flash_player.exe dal sito 1dnscontrol[.]com. Il sito utilizzato per la diffusione (delivery) del *dropper*[1] del codice malevolo **hxxp://1dnscontrol[.]com**. e, in particolare, nelle cartelle */index.php* e */flash_install.php*. avente indirizzo IP ***5.61.37.209*** localizzato in Germania.

Nella tabella seguente sono riportati i domini legati a *1dnscontrol[.]com* contenente il codice malevolo:

Resolve	First	Last
ns1.1dnscontrol.com	22/03/2016 09:38	26/10/2017 02:25
fastmonitor1.net	06/06/2014 19:55	25/10/2017 21:20
www.fastmonitor1.net	31/05/2015 08:08	25/10/2017 10:38
ns2.fastmonitor1.net	17/10/2017 10:43	25/10/2017 10:38
smtp.fastmonitor1.net	17/10/2017 10:44	25/10/2017 10:38
pop.fastmonitor1.net	17/10/2017 10:44	25/10/2017 10:38
ftp.fastmonitor1.net	10/08/2017 10:04	25/10/2017 10:38

[1] **Droppers** sono programmi che installano segretamente programmi malevoli. In genere, i programmi lasciati sul computer della vittima vengono salvati e lanciati senza alcuna notifica (o può essere visualizzata una falsa notifica). I Droppers sono usati per installare segretamente altri malware o per aiutare i programmi malevoli a sfuggire alla rilevazione (non tutti i programmi anti-malware sono in grado di eseguire la scansione di tutti i componenti all'interno di un dropper)

ns1.fastmonitor1.net	17/10/2017 10:44	25/10/2017 10:38
1dnscontrol.com	24/03/2016 00:00	25/10/2017 00:00
mail.1dnscontrol.com	17/10/2017 02:46	24/10/2017 18:52
ftp.1dnscontrol.com	14/08/2017 23:27	24/10/2017 18:52
mail.fastmonitor1.net	18/10/2016 17:50	24/10/2017 18:19
smtp.1dnscontrol.com	17/10/2017 02:45	17/10/2017 02:45
pop.1dnscontrol.com	17/10/2017 02:45	17/10/2017 02:45
openmonitor1.net	05/08/2013 03:16	27/12/2015 02:32
www.openmonitor1.net	30/06/2015 00:03	30/06/2015 00:03

Tabella 1 - Domini legati 1dnscontrol[.]com

Date scanned	Detections	URL
2017-10-26	2/64	http://5.61.37.209/
2017-10-27	1/64	http://fastmonitor1.net/
2017-10-25	1/63	http://5.61.37.209/flash_install.php
2017-10-27	1/64	http://www.fastmonitor1.net/
2017-10-29	13/66	http://1dnscontrol.com/flash_install.php
2017-10-29	14/65	http://1dnscontrol.com/
2017-10-27	13/65	http://1dnscontrol.com/install_flash_player.exe
2017-10-27	8/64	http://ns1.1dnscontrol.com/
2017-10-29	13/65	http://1dnscontrol.com/index.php
2017-10-25	7/64	http://1dnscontrol.com/flash_install.php.
2017-10-24	0/64	http://www.fastmonitor1.net/flash_install.php
2017-10-26	2/64	http://5.61.37.209/

Figure 4- Risultati scansioni degli host legati all'infezione

Downloaded Files

Date scanned	Detections	File type	Name
2017-10-29	57/68	Win32 EXE	Adobe® Flash® Player Installer/Uninstaller 27.0
2017-10-12	0/58	HTML	usaateam.html

Figure 5 - Malware rilevato presso il dominio 1dnscontrol[.]com

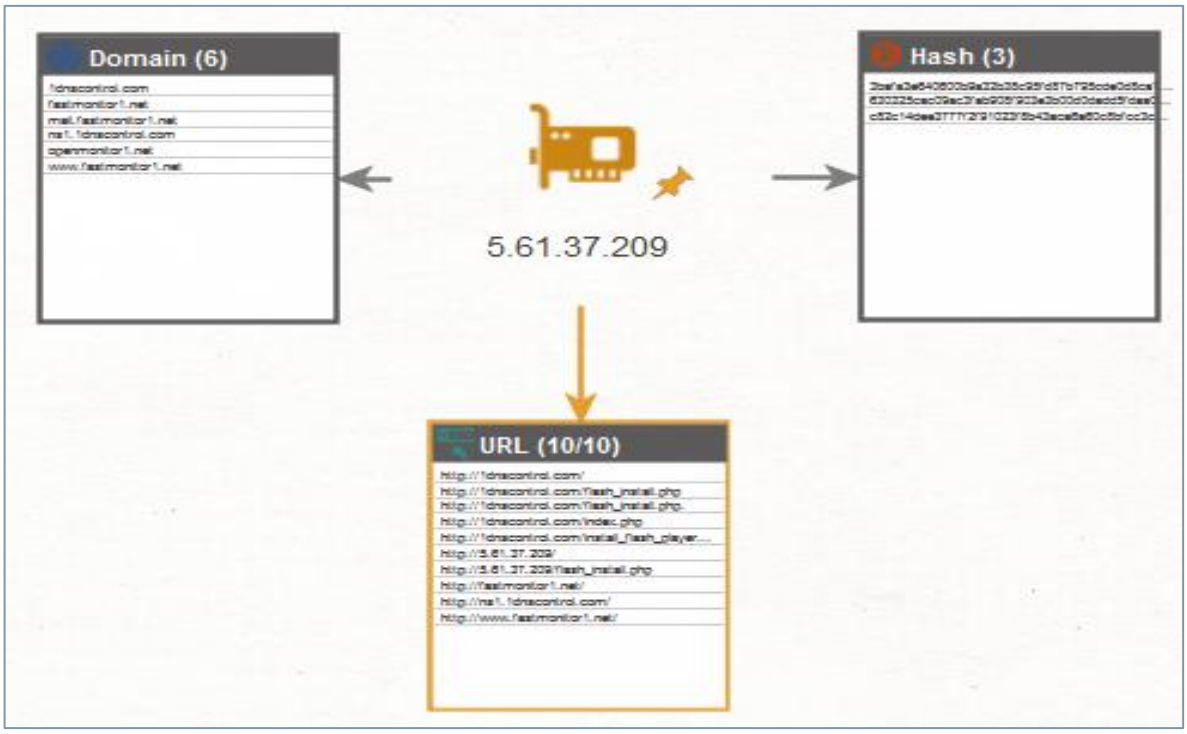

Figure 6 - Risultati scansioni degli host legati all'infezione

http://1dnscontrol.com/
http://1dnscontrol.com/flash_install.php
http://1dnscontrol.com/flash_install.php.
http://1dnscontrol.com/index.php
http://1dnscontrol.com/install_flash_player.exe
http://5.61.37.209/
http://5.61.37.209/flash_install.php
http://fastmonitor1.net/
http://ns1.1dnscontrol.com/
http://www.fastmonitor1.net/

Figure 7 - URL associati al dominio 1dnscontrol[.]com

3bafa3e640600b9a32b38c95fd87b795cde0d8ca73ed3561d8434ece6f67d674
630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da
c82c14dee3777f2f91023f8b43aca6a60c8bfcc3c32e46c320901b5885d8065c

Figure 8 - Codici malevoli che sono attualmente rilevati dalla scansione del dominio 1dnscontrol[.]com

Il dropper, una volta avviato sul computer della vittima, svolge l'estrazione e l'esecuzione del payload del ransmware:

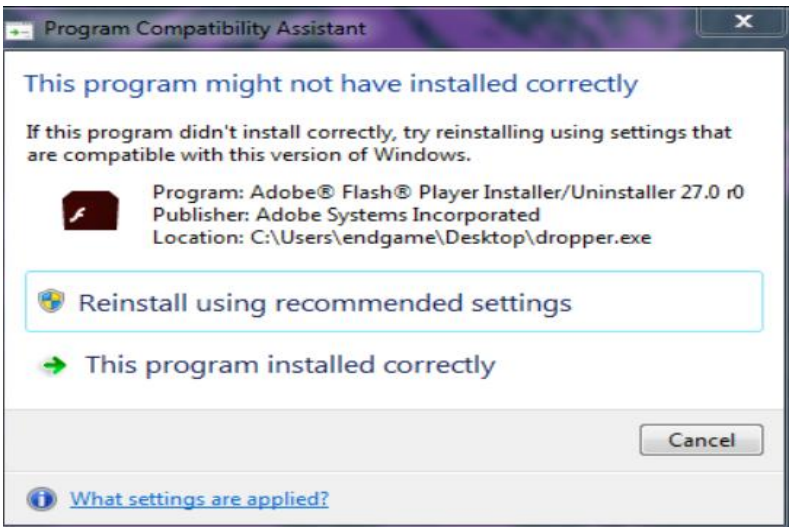

Figure 9 - Messaggio di installazione di Adobe Flash

Il dropper inizialmente utilizzato aveva impronta hash SHA-256 *630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da*. L'archivio è composto dai seguenti file:

- *"C:\Windows\infpub.dat"*
- *"C:\Windows\cscc.dat"*
- *"C:\Windows\dispci.exe"*
- *"C:\Windows\EC95.tmp"*

In particolare, i codici binari (compressi con la libreria *zlib*) contenuti nella sezione *resources* dell'eseguibile che sono memorizzati nella cartella *C:\Windows*:

- Il codice associato con *DiskCryptor* (driver per le architetture x86 e x64 e un client);
- Il codice che realizza un attacco *Mimikatz* per le architetture x86 e x64

L'esecuzione del codice malevolo richiede che l'utente del computer compromesso abbia elevate privilegi e usa Windows UAC per ottenerlo.

La realizzazione delle comunicazioni tra i vari binari è basata su *pipe* nominali, come -ad esempio- la pipe *C:\WINDOWS\561D.tmp* *\\.\pipe\{C1F0BF2D-8C17-4550-AF5A-65A22C61739C}*, mentre per eseguire *infpub.dat* (componente incaricato della cifratura dei file) il malware sfrutta il programma di sistema RunDLL32.exe che è utilizzato per il caricamento e l'esecuzione delle librerie dinamiche *.dll*.

Il malware crea quindi un'operazione pianificata con i parametri mostrati nella schermata seguente:

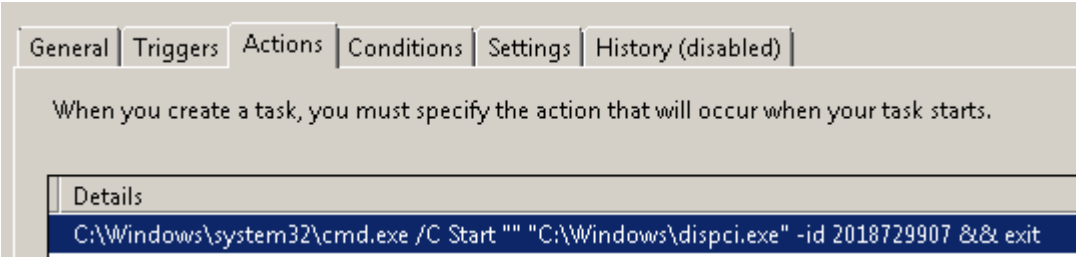

Figure 10 - Creazione di un task pianificato per l'esecuzione dell'eseguibile dispci.exe

La fase di cifratura si basa su due tecniche distinte:

1. *Full disk encryption* con *DiskCryptor* (basato su un codice open source) che esegue anche le modifiche al bootloader per evitare che il sistema esegua il normale processo di booting
2. Cifratura dei singoli file sulla base della loro estensione

La lista delle estensioni interessate alla fase di cifratura è la seguente:

.3ds .7z .accdb .ai .asm .asp .aspx .avhd .back .bak .bmp .brw .c .cab .cc .cer .cfg .conf .cpp .crt .cs .ctl .cxx .dbf .der .dib .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .hpp .hxx .iso .java .jfif .jpe .jpeg .jpg .js .kdbx .key .mail .mdb .msg .nrg .odc .odf .odg .odi .odm .odp .ods .odt .ora .ost .ova .ovf .p12 .p7b .p7c .pdf .pem .pfx .php .pmf .png .ppt .pptx .ps1 .pst .pvi .py .pyc .pyw .qcow .qcow2 .rar .rb .rtf .scm .sln .sql .tar .tib .tif .tiff .vb .vbox .vbs .vcb .vdi .vfd .vhd .vhdx .vmc .vmdk .vmsd .vmtm .vmx .vsdx .vsv .work .xls .xlsx .xml .xvd .zip

La fase di cifratura avviene al rebooting del computer della vittima che viene garantita attraverso la sua schedulazione:

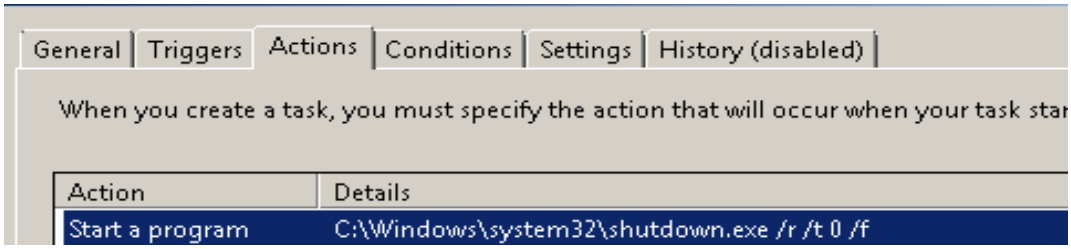

Figure 11 - Creazione di un task pianificato per l'esecuzione del reboot del sistema

Successivamente al reboot del computer viene visualizzata la seguente schermata:

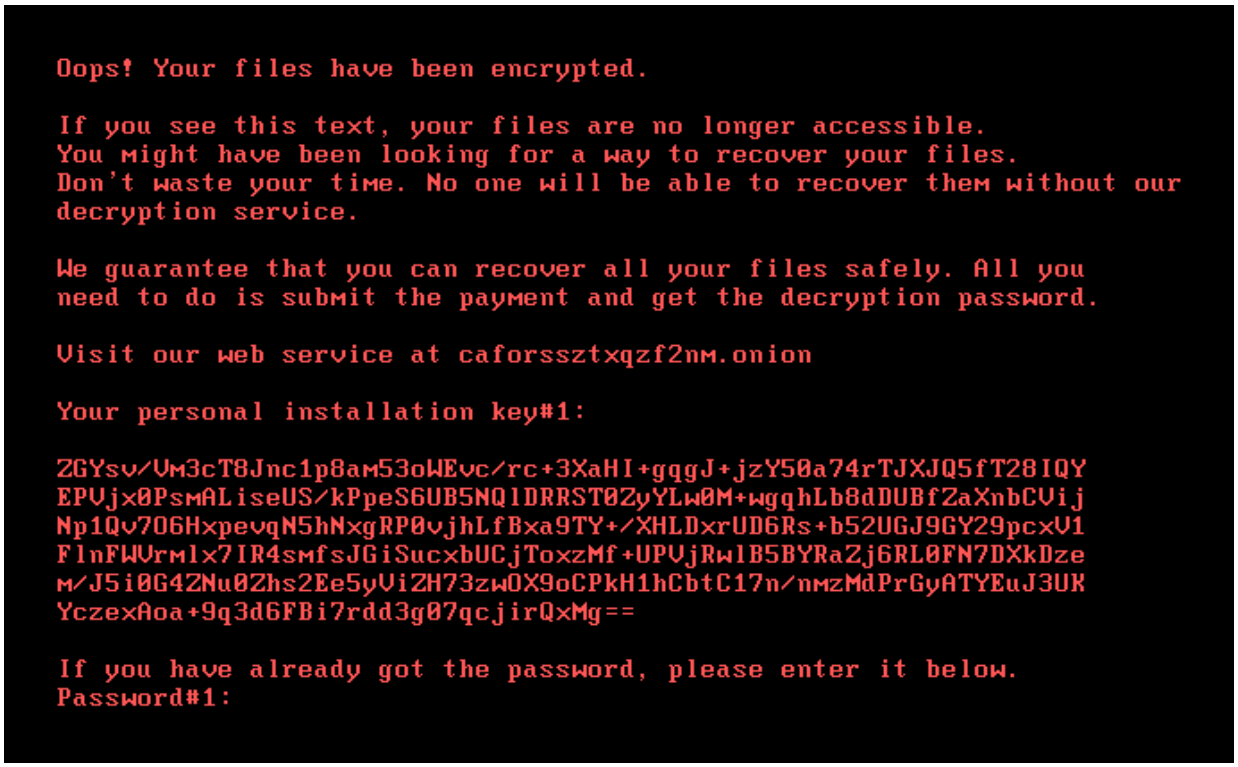

Figure 12 - Schermata con la richiesta del riscatto mostrata all'utente dopo il reboot del Sistema

Figure 13 - Messaggio all'utente che indica il tempo rimanente per effettuare il pagamento senza ulteriori rincari

Il dropper del ransomware è attualmente riconosciuto come malevolo da 53/66 Antivirus engine (alla data del 29 ottobre 2017):

Detection | Details | Relations | Community 10

Ad-Aware	Trojan.GenericKD.6139887	AegisLab	Troj.Ransom.W32.Genic
AhnLab-V3	Trojan/Win32.Diskcoder.R211512	ALYac	Trojan.Ransom.BadRabbit
Antiy-AVL	Trojan/Win32.TSGeneric	Arcabit	Trojan.Generic.D5DAFEF
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Diskcoder.ezxim	AVware	Trojan.Win32.GenericIBT
BitDefender	Trojan.GenericKD.6139887	Bkav	W32.RsRabND.Worm
CAT-QuickHeal	Ransom.BadRabbit.C5	ClamAV	Win.Dropper.Diskcoder-6355411-0
CrowdStrike Falcon	malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	W32/DiskCoder.A.gen!Eldorado	DrWeb	Trojan.BadRabbit.2
eGambit	ransom.BadRabbit	Emsisoft	Trojan-Ransom.BadRabbit (A)
Endgame	malicious (high confidence)	eScan	Trojan.GenericKD.6139887
ESET-NOD32	a variant of Win32/Diskcoder.D	F-Prot	W32/DiskCoder.A.gen!Eldorado
F-Secure	Trojan:W32/Rabbad.A	Fortinet	W32/Diskcoder.Dltr.ransom
GData	Win32.Trojan-Ransom.BadRabbit.C	Ikarus	Trojan-Ransom.BadRabbit
Jiangmin	Trojan.BadRabbit.d	K7AntiVirus	Trojan (0051a3031)
K7GW	Trojan (0051a3031)	Kaspersky	Trojan-Ransom.Win32.BadRabbit.a
Malwarebytes	Ransom.BadRabbit	MAX	malware (ai score=100)
McAfee	RDN/Generic.com	McAfee-GW-Edition	RDN/Generic.com
Microsoft	Ransom:Win32/Tibbar.A	NANO-Antivirus	Trojan.Win32.BadRabbit.euhxbd
nProtect	Ransom/W32.BadRabbit.441899	Palo Alto Networks	generic.ml
Panda	W32/Ransom.G.worm	Qihoo-360	Win32.Ransom.BadRabbit
Sophos AV	Troj/Ransom-ERK	Sophos ML	heuristic
Symantec	Ransom.BadRabbit	Tencent	Win32.Trojan.Badrabbit.Svnz
TrendMicro-HouseCall	Ransom_BADRABBIT.A	VBA32	Trojan.BadRabbit
VIPRE	Trojan.Win32.GenericIBT	ViRobot	Trojan.Win32.S.Ransom.441899
Webroot	W32.Adware.Gen	Yandex	Trojan.Diskcoder!
ZoneAlarm	Trojan-Ransom.Win32.BadRabbit.a	Avast Mobile Security	Clean
Baidu	Clean	CMC	Clean
Comodo	Clean	Cybereason	Clean
Kingsoft	Clean	SentinelOne	Clean
SUPERAntiSpyware	Clean	TheHacker	Clean
WhiteArmor	Clean	Zillya	Clean
Zoner	Clean	Alibaba	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

Figure 14 - Detection del Dropper

Dalle evidenze sinora raccolte, la diffusione del ransomware in un network avviene attraverso la sua duplicazione sfruttando il servizio di Windows Management Instrumentation (WMI) e il Service Control Manager Remote Protocol. Inoltre il ransomware implementa le funzionalità per realizzare l'attacco Mimikatz per trovare le credenziali degli utenti dei sistemi nella stessa network. Inoltre il codice malevolo contiene una lista di credenziali riportati in allegato.

Se falliscono gli attacchi *bruteforce*, allora il malware utilizza l'exploit *EternalRomance* che si basa su una vulnerabilità del protocollo SMB risolta nel MS17-0102. In particolare, il ransomware esegue una scansione sui sistemi appartenenti alla stessa rete alla ricerca di condivisioni SMB e le condivisioni ricercate sono le seguenti:

- admin
- atsvc
- browser
- eventlog
- lsarpc
- netlogon
- ntsvcs
- spoolss
- samr
- srvsvc
- scerpc
- svcctl
- wkssvc

[2] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

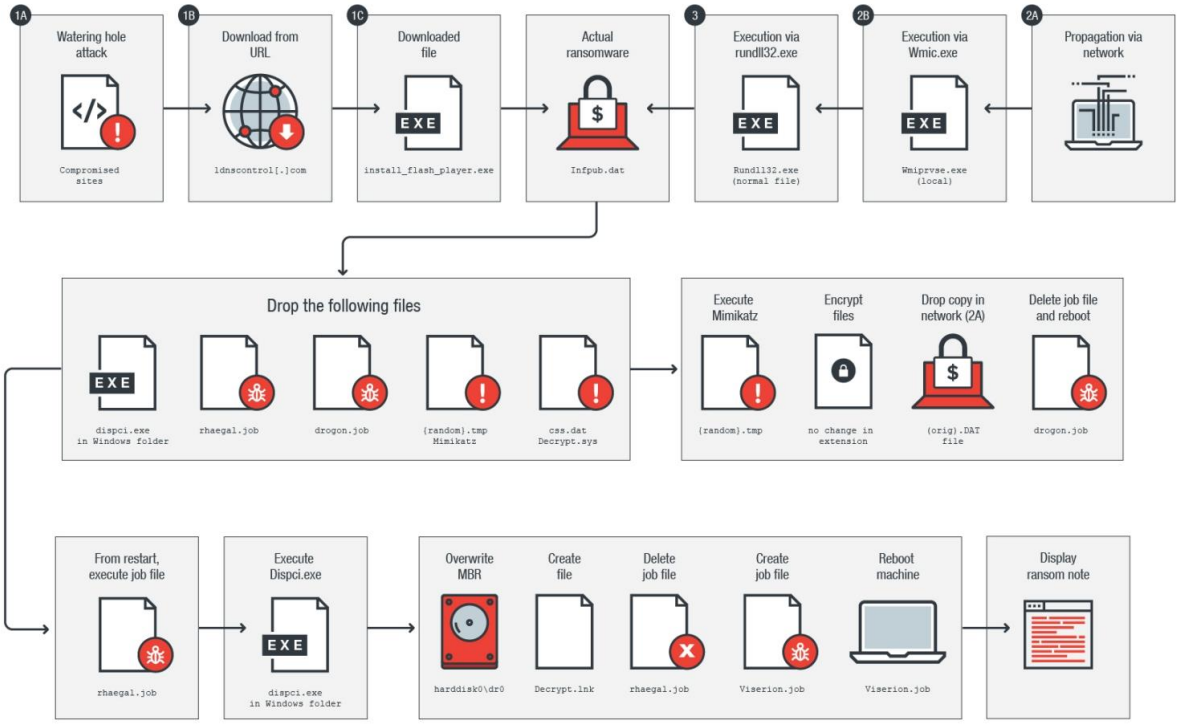

Figure 15 - Flusso logico dell'infezione del ransomware Bad Rabbit

Componenti della campagna di infezione del ransomware Bad Rabbit:

- **Samples**

SHA-1	Filename	Description
79116fe99f2b421c52ef64097f0f39b815b20907	infpub.dat	Diskcoder
afeee8b4acff87bc469a6f0364a81ae5d60a2add	dispci.exe	Lockscreen
413eba3973a15c1a6429d9f170f3e8287f98c21c		Mimikatz (32-bits)
16605a4a29a101208457c47ebfde788487be788d		Mimikatz (64-bits)
de5c8d858e6e41da715dca1c019df0bfb92d32c0	install_flash_player.exe	Dropper
4f61e154230a64902ae035434690bf2b96b4e018	page-main.js	JavaScript on compromised sites

- **C&C servers**

  Payment site: hxxp://caforssztxqzf2nm[.]onion

  Inject URL: hxxp://185.149.120[.]3/scholargoogle/

  Distribution URL: hxxp://1dnscontrol[.]com/flash_install.php

- **Scheduled Tasks names:**

  Viserion

  Rhaegal

  Drogon

SIMILITUDINE TRA IL RANSOMWARE BAD RABBIT E NOTPETYA

L'analisi ha stabilito che «Bad Rabbit» è una versione modificata di NotPetya avente il medesimo algoritmo di crittografia.

NotPetya conteneva lo stesso metodo di crittografia del calcolo della somma di hash a seconda del nome del processo, la differenza consiste nel fatto che il vettore di inizializzazione in NotPetya è 0x12345678, mentre in «Bad Rabbit» è 0x87654321. Inoltre, in questo nuovo attacco la funzione di calcolo della somma è stata compilata come funzione separata.

La società Group-IB sostiene che il l'attacco "Bad Rabbit" abbia delle connessioni con il Bad Actor BlackEnergy.

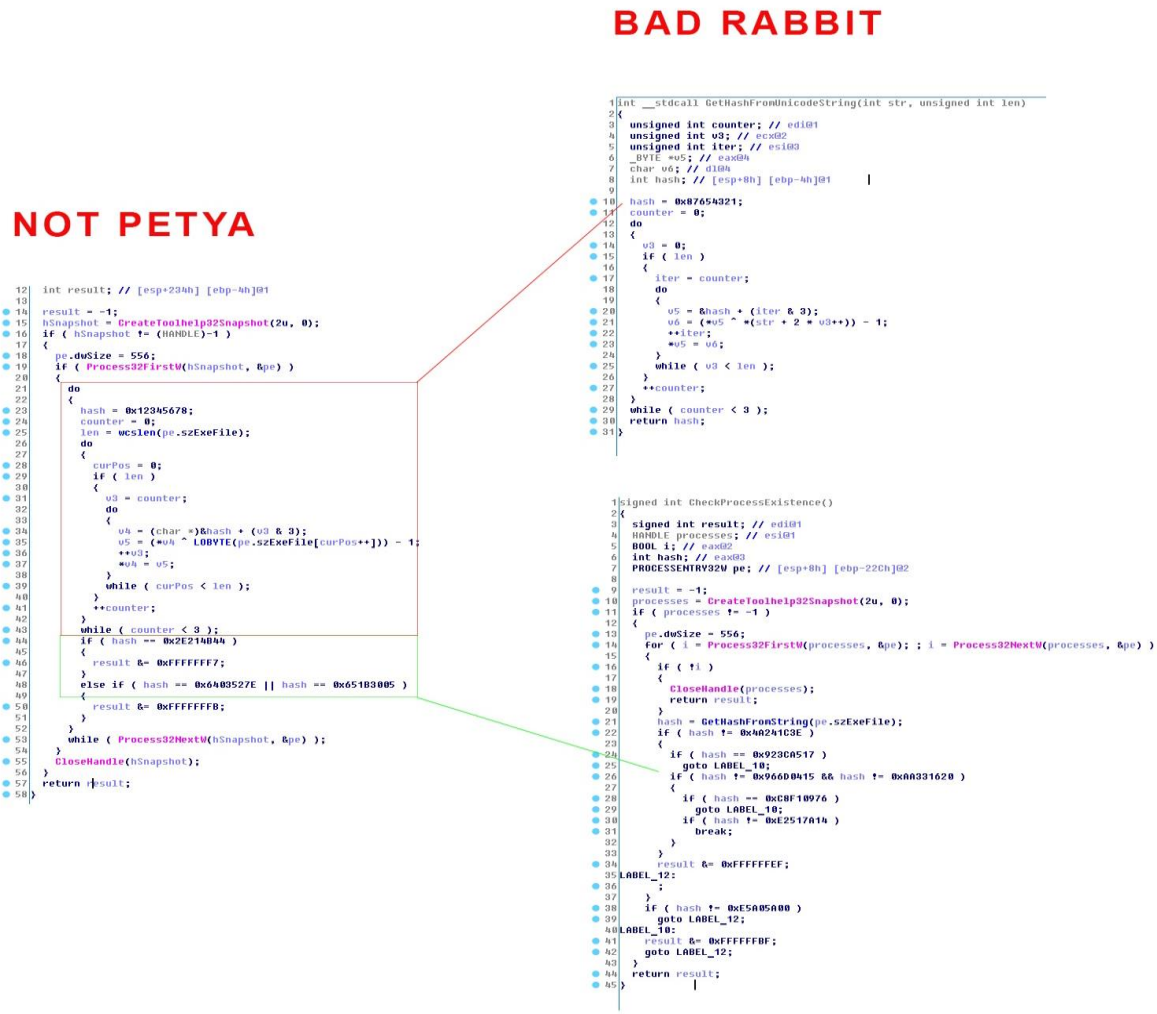

Figure 16 - Porzione di codice comune tra NotPetya e BadRabbit

RACCOMANDAZIONI PER GLI ASPETTI DI PREVENZIONE

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

- 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/

- Creare il *killswitch* legato a questo ransomware creando un file con nome *infpub.dat* nella cartella C:\Windows\. In caso di infezione, il file non sarà crittografato;
- Avviare una attività di scansione dei dischi locali e delle cartelle di rete condivise (anche utilizzando la regola Yara riportata sotto) 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, limitando le attività di schedulazione di : *viserion_, rhaegal, drogon*;
- Verificare il livello di aggiornamento dei sistemi operativi e i sistemi di sicurezza ed effettuare una attività di Patch Management;
- Verificare quali sistemi sono stati impattati ed isolarli dal resto della rete;
- Inserire la lista degli indirizzi IP e nomi di dominio ritenuti malevoli all'interno dei propri sistemi di sicurezza Firewall, IDS, SIEM, etc;
- Disabilitare l'esecuzione automatica degli script e popup, in ogni caso, non collegarsi ai domini indicati come malevoli.
- Utilizzare sistemi automatici come sandbox per l'analisi dei file reputati malevoli.
- 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. Gli utenti di rete devono password robuste;
- Verificare che i dati di backup siano sempre disponibili attraverso test realizzati su base regolare di Recovery ed eseguire il backup di dati importanti;
- 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.

Indicatori di Compromissione (IoC)

Type	Description
Bitcoin wallet	1GxXGMoz7HAVwRDZd7ezkKipY4DHLUqzmM
Bitcoin wallet	17GhezAiRhgB8DGArZXBkrZBFTGCC9SQ2Z
CnC	http://caforssztxqzf2nm.onion/
Domain	argumenti.ru
Domain	an-crimea.ru
Domain	fontanka.ru
Domain	argumentiru.com
Domain	grupovo.bg
Domain	sinematurk.com
Domain	aica.co.jp
Domain	spbvoditel.ru
Domain	mediaport.ua
Domain	www.t.ks.ua
Domain	most-dnepr.info
Domain	osvitaportal.com.ua
Domain	otbrana.com
Domain	pensionhotel.cz
Domain	online812.ru
Domain	imer.ro
Domain	novayagazeta.spb.ru
Domain	i24.com.ua
Domain	ankerch-crimea.ru
Domain	1dnscontrol.com
Domain	webcheck01.net
Domain	webdefense1.net
Domain	secure-check.host
Domain	firewebmail.com
Domain	secureinbox.email
Domain	secure-dns1.net
HASH	79116fe99f2b421c52ef64097f0f39b815b20907
HASH	afeee8b4acff87bc469a6f0364a81ae5d60a2add
HASH	413eba3973a15c1a6429d9f170f3e8287f98c21c
HASH	16605a4a29a101208457c47ebfde788487be788d
HASH	de5c8d858e6e41da715dca1c019df0bfb92d32c0

HASH	4f61e154230a64902ae035434690bf2b96b4e018
IP	185.149.120.3
IP	5.61.37.209

Artefact associati al Ransomware

Modifiche ai registry di sistema

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ Services \ CSCC \ "the DisplayName" = "Windir Client Side DDriver the Caching"

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ Services \ CSCC \ "the ImagePath" = "cscc.dat"

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ cscc \ "Type" = " 1"

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ Services \ CSCC \ "ErrorControl" = "3"

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ Services \ CSCC \ "Etpu Start" = "0"

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ Services \ CSCC \ "DependOnGroup" = ""

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ Services \ CSCC \ "Group is" = "the Filter"

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ cscc \ "DependOnService" = "FltMgr"

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ the Control \ Class \ {4D36E965-E325-11CE-BFC1-08002BE10318} \ "the UpperFilters" = "CSCC"

HKEY_LOCAL_MACHINE \ the SYSTEM \ CurrentControlSet \ the Control \ Class \ {71A27CDD-812A-11D0-BEC7-08002BE2092F} \ "LowerFilters" = "cscc"

Scheduled tasks:

schtasks / the Create / RU the SYSTEM / SC OnStart / TN rhaegal / TR "% the SYSTEM% \ cmd.exe / Etpu Start the C \" \ "\"% Windir% \ dispci.exe \ "-id [NUMBER] && exit "

schtasks / Create / SC once / TN drogon / RU SYSTEM / TR" SYSTEM%% \ shutdown.exe / r / t 0 / f "/ ST [TIME] Using wevtutil malware cleans the following journals:

Trojan deletes the USN journal.

Networking and communication:

hxxt: //caforssztxqzf2nm.onion/ - payment site

hxxt: //185.149.120.3/scholargoogle/ - the URL web of Injection

hxxt: //1dnscontrol.com/flash_install.php - site- distributor

hxxt: // webcheck01.net xxxx: // webdefense1.net

hxxt: // secure-check.host

hxxt: // firewebmail.com

hxxt: // secureinbox.email

hxxt: // secure-dns1.net The BTC: 1GxXGMoz7HAVwRDZd7ezkKipY4DHLUqzmM 17GhezAiRhgB8DGArZXBkrZBFTGCC9SQ2Z

Lista dei siti web attualmente compromessi

hxxp://argumentiru[.]com

hxxp://www.fontanka[.]ru

hxxp://grupovo[.]bg

hxxp://www.sinematurk[.]com

hxxp://www.aica.co[.]jp

hxxp://spbvoditel[.]ru

hxxp://argumenti[.]ru

hxxp://www.mediaport[.]ua

hxxp://blog.fontanka[.]ru

hxxp://an-crimea[.]ru

hxxp://www.t.ks[.]ua

hxxp://most-dnepr[.]info

hxxp://osvitaportal.com[.]ua

hxxp://www.otbrana[.]com

hxxp://calendar.fontanka[.]ru

hxxp://www.grupovo[.]bg

hxxp://www.pensionhotel[.]cz

hxxp://www.online812[.]ru

hxxp://www.imer[.]ro

hxxp://novayagazeta.spb[.]ru

hxxp://i24.com[.]ua

hxxp://bg.pensionhotel[.]com

hxxp://ankerch-crimea[.]ru

Yara Rule Set

```
  Author: Florian Roth
  Date: 2017-10-25
  Identifier: BadRabbit
  Reference: https://pastebin.com/Y7pJv3tK
*/

rule BadRabbit_Gen {
  meta:
    description = "Detects BadRabbit Ransomware"
    author = "Florian Roth"
    reference = "https://pastebin.com/Y7pJv3tK"
    date = "2017-10-25"
    hash1 = "8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93"
    hash2 = "579fd8a0385482fb4c789561a30b09f25671e86422f40ef5cca2036b28f99648"
    hash3 = "630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da"
  strings:
    $x1 = "schtasks /Create /SC ONCE /TN viserion_%u /RU SYSTEM /TR \"%ws\" /ST" fullword wide
    $x2 = "schtasks /Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR \"%ws /C Start \\\"\\\" \\\"%wsdispci.exe\\\"" fullword wide
    $x3 = "C:\\Windows\\infpub.dat" fullword wide
    $x4 = "C:\\Windows\\cscc.dat" fullword wide

    $s1 = "need to do is submit the payment and get the decryption password." fullword ascii
```

```
    $s2 = "\\\\.\\GLOBALROOT\\ArcName\\multi(0)disk(0)rdisk(0)partition(1)"
fullword wide
    $s3 = "\\\\.\\pipe\\%ws" fullword wide
    $s4 = "fsutil usn deletejournal /D %c:" fullword wide
    $s5 = "Run DECRYPT app at your desktop after system boot" fullword ascii
    $s6 = "Files decryption completed" fullword wide
    $s7 = "Disable your anti-virus and anti-malware programs" fullword wide
    $s8 = "SYSTEM\\CurrentControlSet\\services\\%ws" fullword wide
    $s9 = "process call create \"C:\\Windows\\System32\\rundll32.exe" fullword wide
    $s10 = "%ws C:\\Windows\\%ws,#1 %ws" fullword wide
  condition:
    uint16(0) == 0x5a4d and filesize < 700KB and ( 1 of ($x*) or 2 of them )
}

rule BadRabbit_Mimikatz_Comp {
  meta:
    description = "Auto-generated rule - file
2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035"
    author = "Florian Roth"
    reference = "https://pastebin.com/Y7pJv3tK"
    date = "2017-10-25"
    hash1 = "2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035"
  strings:
    $s1 = "%lS%lS%lS:%lS" fullword wide
    $s2 = "lsasrv" fullword wide
    $s3 = "CredentialKeys" ascii
    /* Primary\x00m\x00s\x00v */
    $s4 = { 50 72 69 6D 61 72 79 00 6D 00 73 00 76 00 }
```

```
  condition:
    ( uint16(0) == 0x5a4d and filesize < 200KB and 3 of them )
}
```

Credenziali incluse nel ransomware

Usernames

Administrator	buh	work	nasuser
Admin	boss	other user	nasadmin
Guest	ftp	operator	superuser
User	rdp	backup	netguest
User1	rdpuser	asus	alex
user-1	rdpadmin	ftpuser	
Test	manager	ftpadmin	
root	support	nas	

Passwords

Administrator	123456	Admin123	qwert
administrator	1234567	admin123Test123	qwerty
Guest	12345678	test123	qwerty123
guest	123456789	password	zxc
User	1234567890	111111	zxc123
user	Administrator123	55555	zxc321
Admin	administrator123	77777	zxcv
adminTest	Guest123	777	uiop
test	guest123	qwe	123321
root	User123	qwe123	321
123	user123	qwe321	love
1234		qwer	secret
12345			sex
god			

DeepCyber Srl
Piazzale Don Luigi Sturzo 15 - Roma
info@deepcyber.it oppure hunting@deepcyber.it
www.deepcyber.it