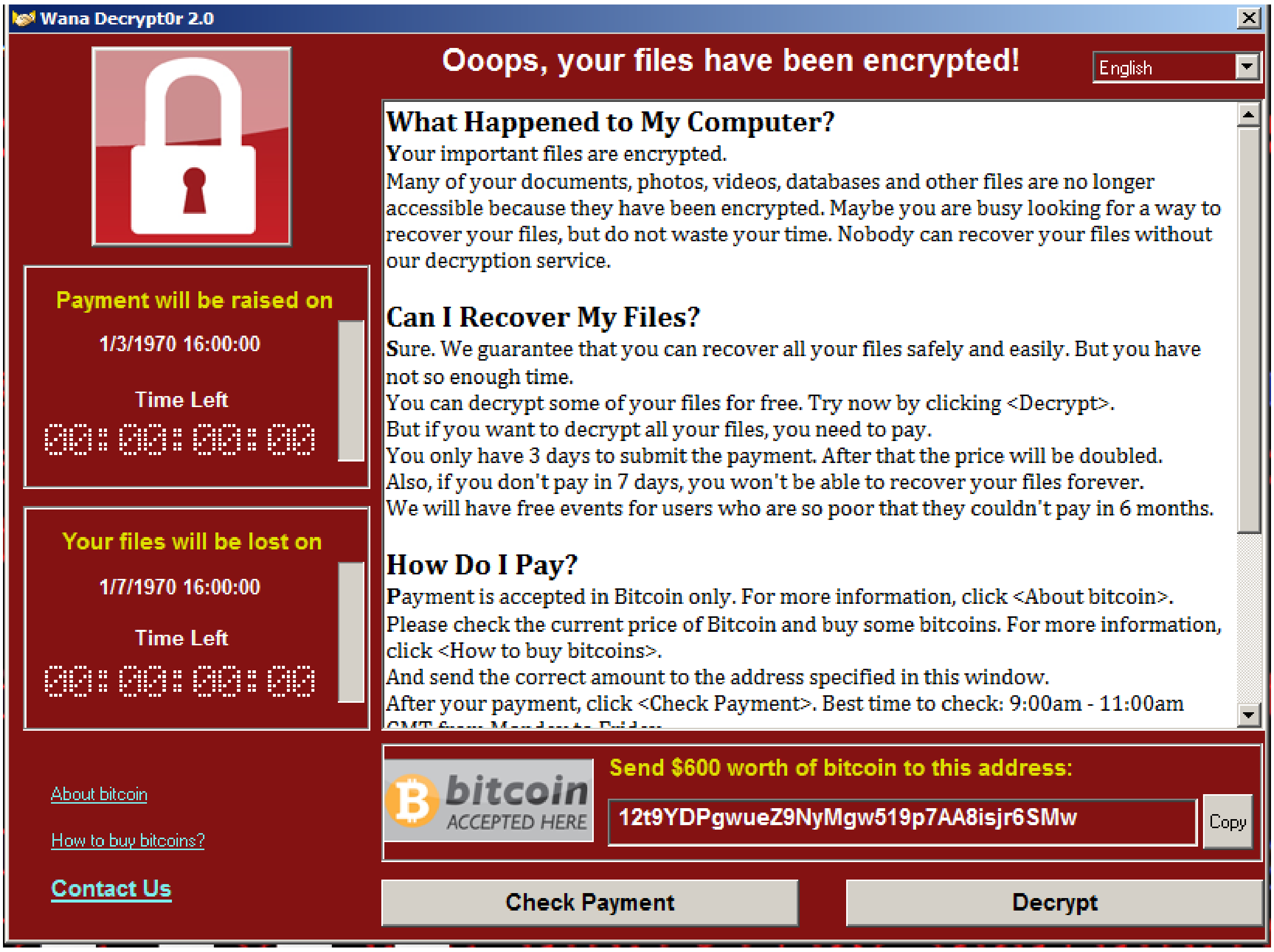
WannaCry Ransomware and MS17-010 Vulnerability

Gal Goldshtein, 2017-16-05

On Friday 12 May 2017 a large ransomware attack dubbed “WannaCry” was launched targeting more than 200,000 computers worldwide, including industries such as banks, hospitals and large telecom companies.



Ooops, your files have been encrypted!

Payment will be raised on
1/3/1970 16:00:00
Time Left
00:00:00:00

Your files will be lost on
1/7/1970 16:00:00
Time Left
00:00:00:00

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $600 worth of bitcoin to this address:

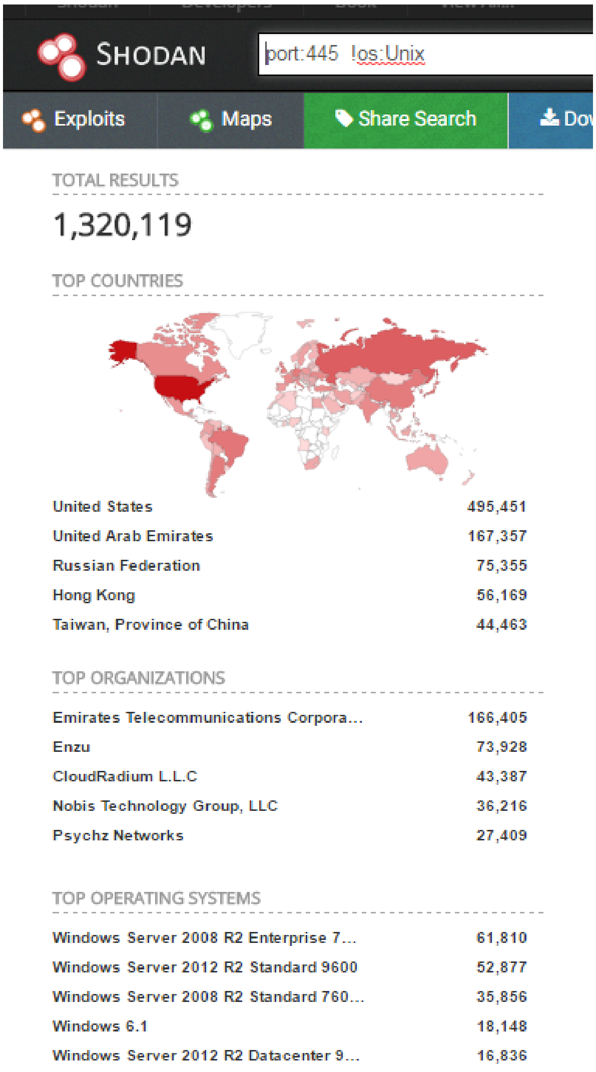
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 1: *“WannaCry” ransom massage*

Infection Methods

One of the main infection methods of this ransomware is by exploiting a recently patched Microsoft Windows SMB vulnerability (MS17-010). This vulnerability was publicly discovered as a result of the Shadow Brokers leaks that happened in April this year. Another possible method of infection is by phishing emails being sent to arbitrary recipients.

Either way, once this ransomware gets on a network it exploits the aforementioned windows vulnerability in order to spread further into the network and infect more computers.



port:445 !os:Unix

TOTAL RESULTS

1,320,119

TOP COUNTRIES

United States	495,451
United Arab Emirates	167,357
Russian Federation	75,355
Hong Kong	56,169
Taiwan, Province of China	44,463

TOP ORGANIZATIONS

Emirates Telecommunications Corpora...	166,405
Enzu	73,928
CloudRadium L.L.C	43,387
Nobis Technology Group, LLC	36,216
Psychz Networks	27,409

TOP OPERATING SYSTEMS

Windows Server 2008 R2 Enterprise 7...	61,810
Windows Server 2012 R2 Standard 9600	52,877
Windows Server 2008 R2 Standard 760...	35,856
Windows 6.1	18,148
Windows Server 2012 R2 Datacenter 9...	16,836

Figure 2: *Shodan search for Windows SMB service exposed directly to the internet*

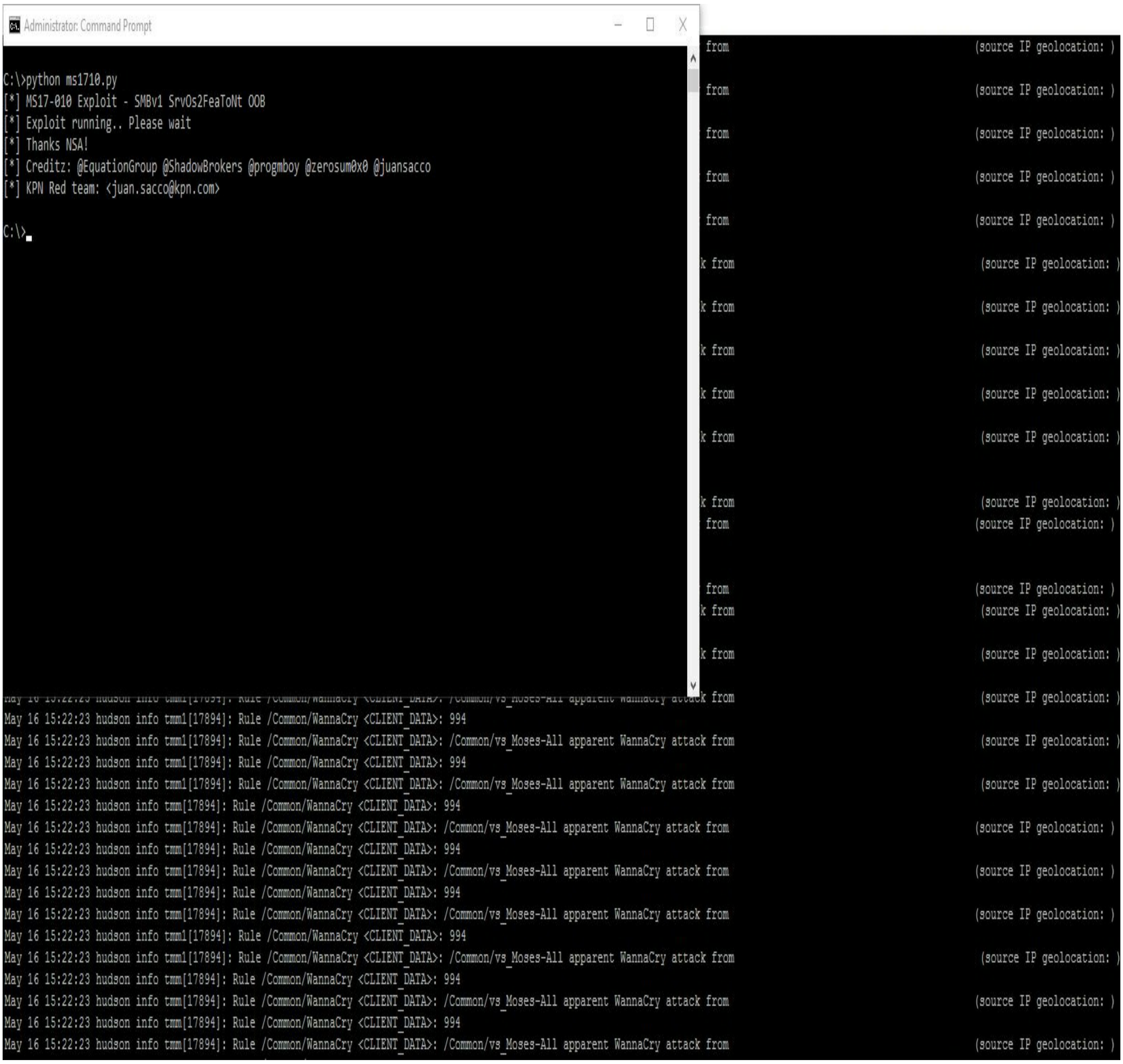
Mitigation using BIG-IP

BIG-IP is able to mitigate the Windows exploitation attempt and prevent the WannaCry ransomware infection by using the attached iApp which contains an iRule, the iRule detects a part of the kernel shellcode in the exploit and drops the packets containing it.

```
sys application template WannaCry_Blocker_v2 {
    actions {
        definition {
            html-help {
<h3>WannaCry Blocker</h3>
<p>This iApp installs the WannaCry Blocker iRule which will detect,
 block,* log, and count attempts to exploit CVE-2017-0144
 &ldquo;WannaCry.&rdquo;</p>
<p>Attach <i><b>both</b></i> the WannaCry Blocker
 iRule <i>and</i> the default Stream Profile /Common/stream to a TCP
 virtual server (the virtual server must not have an HTTP Profile).</p>
<p>The WannaCry Blocker iRule logs the source IP address and geolocation
 of each possible attack and counts attacks (per-virtual-server)
 using iStats.</p>
<p><b>*</b> The WannaCry iRule blocks WannaCry attacks.  It also has an
 option to log attacks then allow them to proceed, if you really want
 to do that.</p>
            }
            implementation {
```

```
            implementation {
package require iapp 1.1.1

iapp::template start

# Prepared by Mark Quevedo, f5 Networks

#------------------------------------------------------------

set ir_wcry {
# WannaCry Blocker iRule
#
# Attach this iRule along with the defaul Stream Profile
# /Common/stream to a TCP virtual server to detect, block,*
# log, and count CVE-2017-0144 "WannaCry" attacks.  (The
# virtual server must not have an HTTP Profile.)
#
# This iRule logs the source IP address and geolocation of each
# attack and counts attacks (per-virtual-server) using iStats.
#
# * Normally this iRule blocks WannaCry attacks.  If you really
# wish to allow such attacks to proceed (to a honeypot, maybe?)
# after they are logged, set the variable static::allow_wannacry
# to '1' in the RULE_INIT event.
#
# Written by Mark Quevedo, f5 Networks
#

when RULE_INIT {
 # if static::allow_wannacry is set to 1 (true) (see next line)
 # then WannaCry attacks are not blocked, just logged and counted
 set static::allow_wannacry @@@@@


 # Stream Profile target sequences here are TCL regular expressions.
 # TMOS maps payload octets as if they were ISO-8859-1 to Unicode chars
 set target_list {
  {\u00b9\u0082\u0000\u0000\u00c0\u000f\u0032\u0048\u00bb\u00f8\u000f\u00d0\u00ff{5}\u0089\u0053\u000
  {\u0010\u0000{4}\u00ff{4}\u0000{12}\u004a\u0000{3}\u004a\u0000\u0002\u0000\u0023\u0000{3}\u0007\u00
 }

 set static::wcry_targets ""
 append static::wcry_targets "/" [join $target_list "// /"] "//"
} ; #RULE_INIT

when CLIENT_ACCEPTED {
 STREAM::expression $static::wcry_targets
 STREAM::enable
} ; #CLIENT_ACCEPTED

when STREAM_MATCHED {
 if {$static::allow_wannacry} {
  STREAM::replace ; # no arg means don't replace, therefore allow
  set blocked ""
 } else {
  reject ; # block apparent WannaCry attack
  set blocked "blocked\x20"
 }
 set client_ip [IP::client_addr]
 set client_port [TCP::client_port]
 set local_ip [IP::local_addr]
 set local_port [TCP::local_port]
 set geo [whereis $client_ip continent country city isp latitude longitude]

 log local0.info "[virtual] ${blocked}apparent WannaCry attack from ${client_ip}_${client_port} to ${

 ISTATS::incr "ltm.virtual [virtual] c wannacry" 1
} ; #STREAM_MATCHED
} ; #ir_wcry

#------------------------------------------------------------

# create/update iRule
regsub -all {@@@@@} $ir_wcry [expr {!$::intro__block}] patched
iapp::conf "create ltm rule WannaCry-Blocker { ${patched} }"

iapp::template end
            }
            presentation {
section intro {
    message note1 "This iApp installs the WannaCry Blocker iRule which will detect, block,* log, and
    message note2 "Attach BOTH the WannaCry Blocker iRule AND the default Stream Profile /Common/stre
    message note3 "The WannaCry Blocker iRule logs the source IP address and geolocation of each poss
    message note4 "* Normally the WannaCry Blocker iRule (WannaCry-Blocker) blocks WannaCry attacks i
    choice block display "xxlarge" {
     "Yes!  Block WannaCry attacks; also log and count them" => "1",
     "No.  Log and count WannaCry attacks but do NOT block them (INSECURE)" => "0"
    }
}

text {
    intro "Welcome to the WannaCry Blocker iApp template v2"
    intro.note1 "Description"
    intro.note2 ""
    intro.note3 ""
    intro.note4 ""
    intro.block "Do you want the WannaCry Blocker iRule to block WannaCry attacks?"
}
            }
            role-acl { admin }
            run-as none
        }
    }
    requires-bigip-version-max none
    requires-bigip-version-min 11.0.0
    requires-modules { ltm }
    description "WannaCry Blocker to detect/block/log/count CVE-2017-0144 'WannaCry' attacks"
}
```

Figure 3: *iApp template for logging and blocking MS17-010 exploitation attempts*



```
C:\>python ms1710.py
[*] MS17-010 Exploit - SMBv1 SrvOs2FeaToNt OOB
[*] Exploit running.. Please wait
[*] Thanks NSA!
[*] Creditz: @EquationGroup @ShadowBrokers @progmboy @zerosum0x0 @juansacco
[*] KPN Red team: <juan.sacco@kpn.com>

C:\>_
```

```
 from                                        (source IP geolocation: )

 from                                        (source IP geolocation: )

 from                                        (source IP geolocation: )

 from                                        (source IP geolocation: )

 from                                        (source IP geolocation: )

k from                                        (source IP geolocation: )

k from                                        (source IP geolocation: )

k from                                        (source IP geolocation: )

k from                                        (source IP geolocation: )

k from                                        (source IP geolocation: )


k from                                        (source IP geolocation: )
 from                                        (source IP geolocation: )


 from                                        (source IP geolocation: )
k from                                        (source IP geolocation: )

k from                                        (source IP geolocation: )

May 16 15:22:23 hudson info tmm1[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm1[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm1[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm1[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm1[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm1[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm1[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: 994
May 16 15:22:23 hudson info tmm[17894]: Rule /Common/WannaCry <CLIENT_DATA>: /Common/vs_Moses-All apparent WannaCry attack from          (source IP geolocation: )
```

Figure 4: *Exploit attempt against BIG-IP which has the iRule configured*

It is important to emphasize that BIG-IP is not vulnerable to this Windows SMB vulnerability as it doesn't run Windows OS.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com