WANNACRY RANSOMWARE ANALYSIS

LogRhythm Labs

May 2017

LogRhythm®

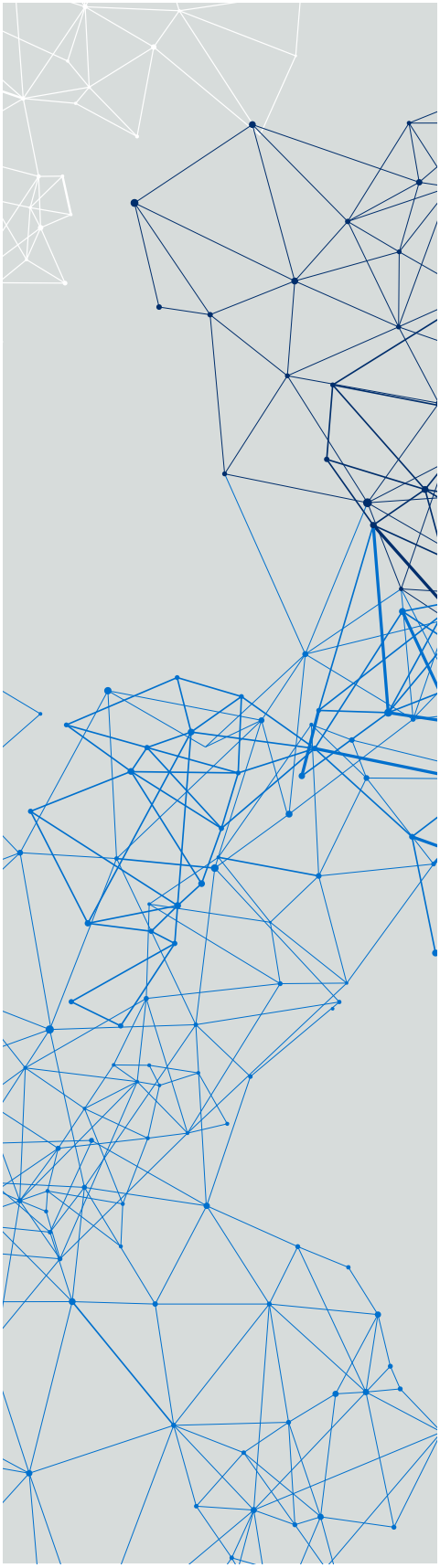
The Security Intelligence Company

Table of Contents

Summary

Ransomware that has been publicly named "WannaCry", "WCry" or "WanaCryptOr" (based on strings in the binary and encrypted files) has spread to at least 74 countries as of Friday 12 May 2017, reportedly targeting Russia initially, and spreading to telecommunications, shipping, car manufacturers, universities and health care industries, among others. The malware encrypts user files, demanding a fee of either $300 or $600 worth of bitcoins to an address specified in the instructions displayed after infection.

The WannaCry ransomware is composed of multiple components. An initial dropper contains the encrypter as an embedded resource; the encrypter component contains a decryption application ("Wana DecryptOr 2.0"), a password-protected zip containing a copy of Tor, and several individual files with configuration information and encryption keys. It is not conclusively known as of this report what vector was used for the initial infection. There was speculation that a weaponized PDF was circulated in a phishing campaign, but analysts have not confirmed this conjecture, and the supposed PDF sample obtained by LogRhythm analysts was not functional.



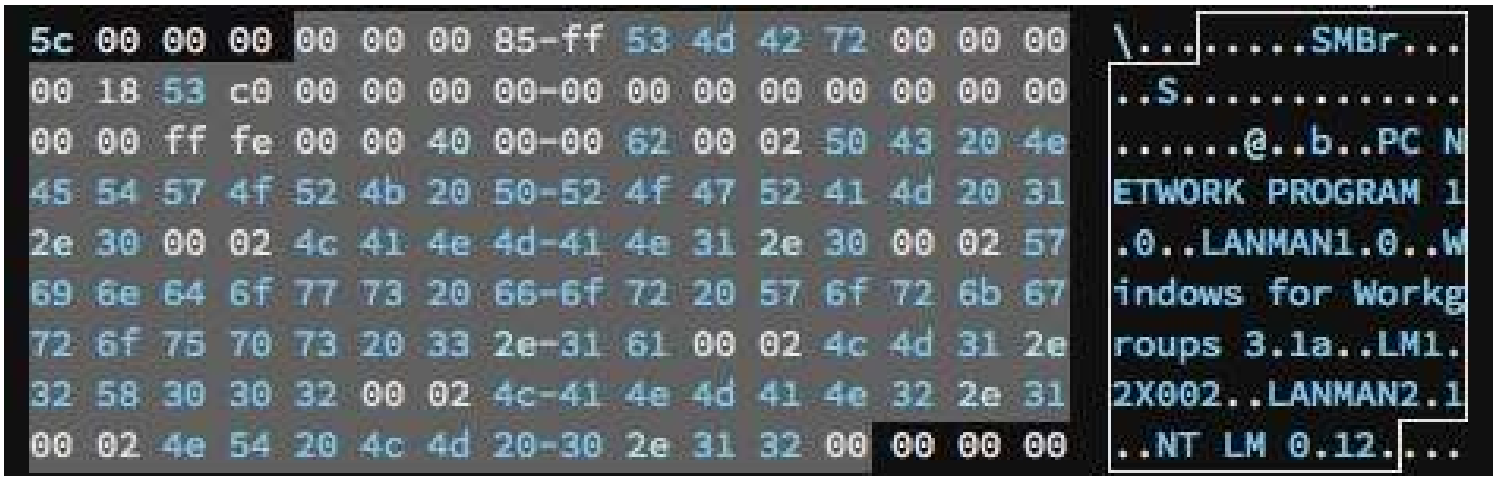
Analysis

Multiple samples of the WannaCry dropper have been identified by researchers. Although they share similar functionality, the samples differ slightly. The dropper sample, encrypter, and decrypter analyzed in this report have the following SHA256 hash values:

Dropper	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Encrypter	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Decrypter	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

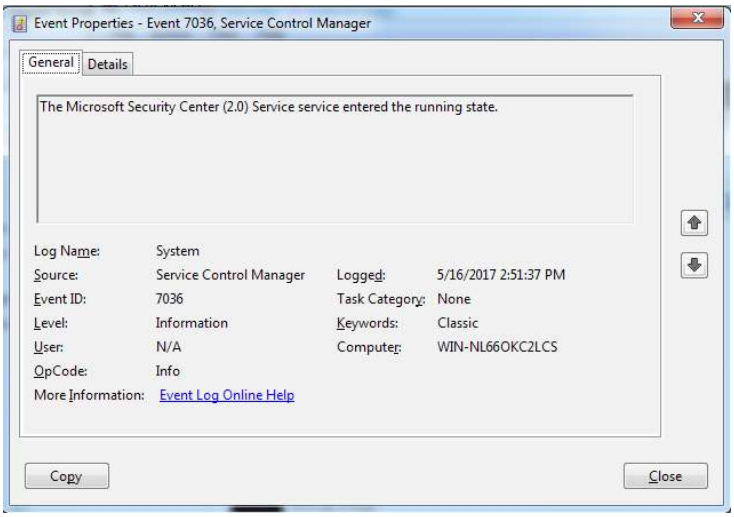
The authors did not appear to be concerned with thwarting analysis, as the samples analyzed have contained little if any obfuscation, anti-debugging, or VM-aware code. However, the malware makes use of an exploit developed by NSA analysts that was patched by Microsoft 14 March 2017 (MS17-010, see https://technet.microsoft.com/en-us/library/security/ms17-010.aspx for details), although there are many unpatched systems still vulnerable. Applying this patch will mitigate the spread of WannaCry, but will not prevent infection.

The exploit used, named EternalBlue, exploits a vulnerability in the Server Message Block (SMB) protocol that allows the malware to spread to all unpatched Windows systems from XP to 2016 on a network that have this protocol enabled. This vulnerability allows remote code execution over SMB v1. WannaCry utilizes this exploit by crafting a custom SMB session request with hard-coded values based on the target system. Notably, after the first SMB packet sent to the victim's IP address, the malware sends two additional packets to the victim containing the hard-coded IP addresses 192.168.56.20 and 172.16.99.5. A LogRhythm Network Monitor query rule to detect this traffic is included at the end of this report.



Sample SMB packet

When the dropper is executed, it first attempts to make a connection to the domain http://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com and exits if the connection is successful. This domain was previously unregistered, causing this connection to fail. However, on the afternoon of May 12, this domain was registered and sinkholed by researcher MalwareTech, effectively acting as a "kill switch" for many systems, and thereby slowing the rate of infection. However, the method by which the malware opens the connection does not affect systems connecting through a proxy server, leaving those systems still vulnerable.



If the connection fails, the dropper attempts to create a service named "mssecsvc2.0" with the DisplayName "Microsoft Security Center (2.0) Service." This can be observed in the System Event Log as event ID 7036, indicating that the service has started.

The dropper then extracts the encrypter binary from its resource R/1831, writes it to the hardcoded filename %WinDir%\tasksche.exe, and then executes it.

When executed, the encrypter checks to see if the mutex "MsWinZonesCacheCounterMutexA" exists, and will not proceed if present.

```
push    offset aGlobalMswinzon ; "Global\\MsWinZonesCacheCounterMutexA"
lea     eax, [ebp+Dest]
push    offset aSD      ; The sprintf format "%s%d" appends a "0" to the end of the mutex name
push    eax             ; Dest
call    ds:sprintf      ; Global\\MsWinZonesCacheCounterMutexA0
xor     esi, esi
add     esp, 10h
cmp     [ebp+arg_0], esi
jle     short loc_401F4C

                        ; CODE XREF: check_mutex+4B↓j
lea     eax, [ebp+Dest]
push    eax             ; lpName
push    1               ; bInheritHandle
push    100000h         ; dwDesiredAccess
call    ds:OpenMutexA   ; Check for existence of mutex
test    eax, eax
jnz     short loc_401F51 ; If this mutex exists, the malware exits
push    1000            ; dwMilliseconds
call    ds:Sleep
inc     esi             ; Increment the counter
cmp     esi, [ebp+arg_0] ; Compares the incrementer to the value 60, effectively
                        ; performing this mutex check each second for one minute
jl      short loc_401F26
```

The encrypter binary also contains a password-protected zip file (password: WNcry@2ol7) containing the following files:

- A directory named "msg" containing Rich Text Format files with the extension .wnry. These files are the "Readme" file used by the @WanaDecryptor@.exe decrypter program in each of the following languages:

bulgarian	english	italian	romanian
chinese (simplified)	filipino	japanese	russian
chinese (traditional)	finnish	korean	slovak
croatian	french	latvian	spanish
czech	german	norwegian	swedish
danish	greek	polish	turkish
dutch	indonesian	portuguese	vietnamese

The English and Spanish translations (at least) of the decryption message appear to be machine-translated, as there are grammatical mistakes that would not be expected from native speakers.

- b.wnry, a bitmap file displaying instructions for decryption
- c.wnry, containing the following addresses:
  - gx7ekbenv2riucmf.onion
  - 57g7spgrzlojinas.onion
  - xxlvbrloxvriy2c5.onion
  - 76jdd2ir2embyv47.onion
  - cwwnhwhlz52maqm7.onion
  - https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip
- r.wnry, additional decryption instructions used by the decrypter tool, in English
- s.wnry, a zip file containing the Tor software executable
- t.wnry, encrypted using the WANACRY! encryption format, where "WANACRY!" is the file header
- taskdl.exe, (hash 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79), file deletion tool
- taskse.exe, (hash 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d), enumerates Remote Desktop Protocol (RDP) sessions and executes the malware on each session
- u.wnry (hash b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25), "@WanaDecryptor@.exe" decrypter file

After dropping these files to its working directory, the malware attempts to change the attributes of all the files to "hidden" and grant full access to all files in the current directory and any directories below. It does this by executing "attrib +h .", followed by "icacls . /grant Everyone:F /T /C /Q".

```
push    ebx             ; lpExitCode
push    ebx             ; dwMilliseconds
push    offset CommandLine ; "attrib +h ."
call    sub_401064
push    ebx             ; lpExitCode
push    ebx             ; dwMilliseconds
push    offset aIcacls_GrantEv ; "icacls . /grant Everyone:F /T /C /Q"
call    sub_401064
```

WannaCry then proceeds to encrypt files on the system, searching for the following file extensions, which are hard-coded in the binary:

.docx	.ppam	.sti	.vcd	.3gp	.sch	.myd	.wb2
.docb	.potx	.sldx	.jpeg	.mp4	.dch	.frm	.slk
.docm	.potm	.sldm	.jpg	.mov	.dip	.odb	.dif
.dot	.pst	.sldm	.bmp	.avi	.pl	.dbf	.stc
.dotm	.ost	.vdi	.png	.asf	.vb	.db	.sxc
.dotx	.msg	.vmdk	.gif	.mpeg	.vbs	.mdb	.ots
.xls	.eml	.vmx	.raw	.vob	.ps1	.accdb	.ods
.xlsx	.edb	.gpg	.cgm	.mpg	.bat	.sql	.3dm
.xlsm	.vsd	.aes	.tif	.wmv	.cmd	.sqlitedb	.max
.xlsb	.vsdx	.ARC	.tiff	.fla	.js	.sqlite3	.3ds
.xlw	.txt	.PAQ	.nef	.swf	.asm	.asc	.uot
.xlt	.csv	.bz2	.psd	.wav	.h	.lay6	.stw
.xlm	.rtf	.tbk	.ai	.mp3	.pas	.lay	.sxw
.xlc	.123	.bak	.svg	.sh	.cpp	.mml	.ott
.xltx	.wks	.tar	.djvu	.class	.c	.sxm	.odt
.xltm	.wk1	.tgz	.m4u	.jar	.cs	.otg	.pem
.ppt	.pdf	.gz	.m3u	.java	.suo	.odg	.p12
.pptx	.dwg	.7z	.mid	.rb	.sln	.uop	.csr
.pptm	.onetoc2	.rar	.wma	.asp	.ldf	.std	.crt
.pot	.snt	.zip	.flv	.php	.mdf	.sxd	.key
.pps	.hwp	.backup	.3g2	.jsp	.ibd	.otp	.pfx
.ppsm	.602	.iso	.mkv	.brd	.myi	.odp	.der
.ppsx	.sxi						

In addition, a registry key is written to "HKLM\SOFTWARE\Wow6432Node\WanaCryptOr\wd" which adds a key to reference the location from which WannaCry was originally executed.

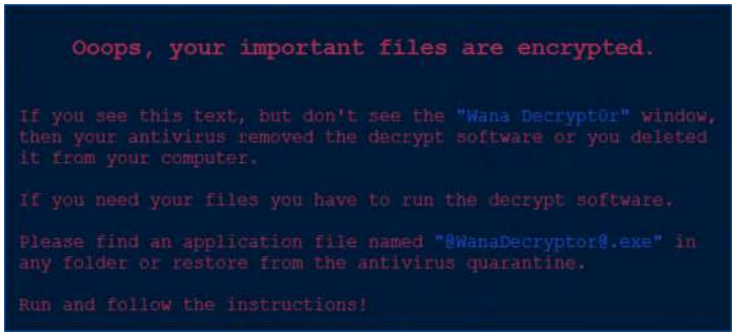
The WannaCry encrypter launches the embedded decrypter binary "@WanaDecryptor@.exe", which displays two timers and instructions for sending the ransom in the configured language of the infected system. The instructions demand a payment of $300 worth of bitcoins to a specified address. The following addresses are hardcoded in the binary, although only the first was observed to be used by the analyzed sample:

- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

```
push    ebp
mov     ebp, esp
sub     esp, 318h
lea     eax, [ebp+var_318]
push    1               ; int
push    eax             ; void *
mov     [ebp+var_C], offset a13am4vw2dhxygx ; "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
mov     [ebp+var_8], offset a12t9ydpgwuez9n ; "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"
mov     [ebp+var_4], offset a115p7ummngoj1p ; "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
call    sub_401000
pop     ecx
```

The following is a screenshot of the "Wana DecryptOr 2.0" program:

The malware also displays the following bitmap image contained in "b.wnry" on the desktop, in case the "Wana DecryptOr" program failed to execute:



If the ransom is not paid before the first timer expires, the ransom price doubles. After the second timer expires, the malware readme states that the files will be unrecoverable. Once the files are encrypted, they are unrecoverable without the decryption key. The malware uses the Microsoft Enhanced RSA and AES Cryptographic Provider libraries to perform the encryption.

After the files are encrypted, the decrypter program attempts to delete any Windows Shadow Copies via this command:

cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet

Mitigation

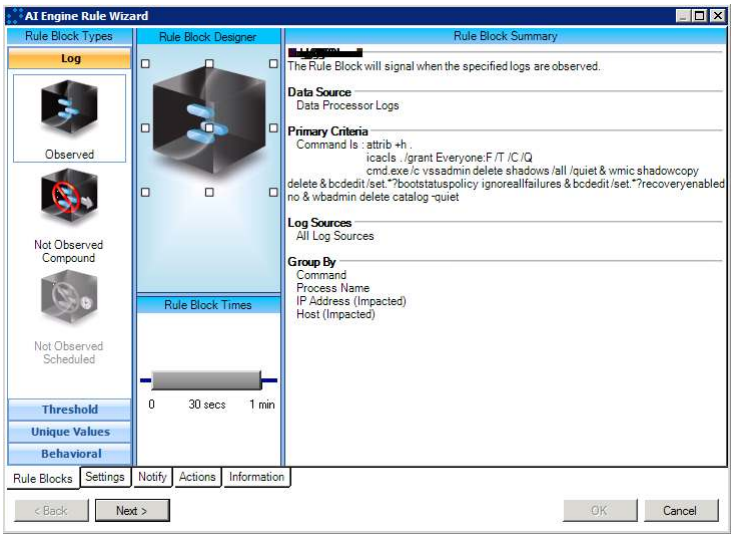
If a system becomes infected with the WannaCry ransomware, it is best to try to restore files from backup rather than paying the ransom, as there is no guarantee that payment will lead to successful decryption.

In order to prevent infection and the spread of this malware across the network, all Windows systems should be up to date on current patches and antivirus signatures. Additionally, blocking inbound connections to SMB ports (139 and 445) will prevent the spread of the malware to systems still vulnerable to the patched exploit.

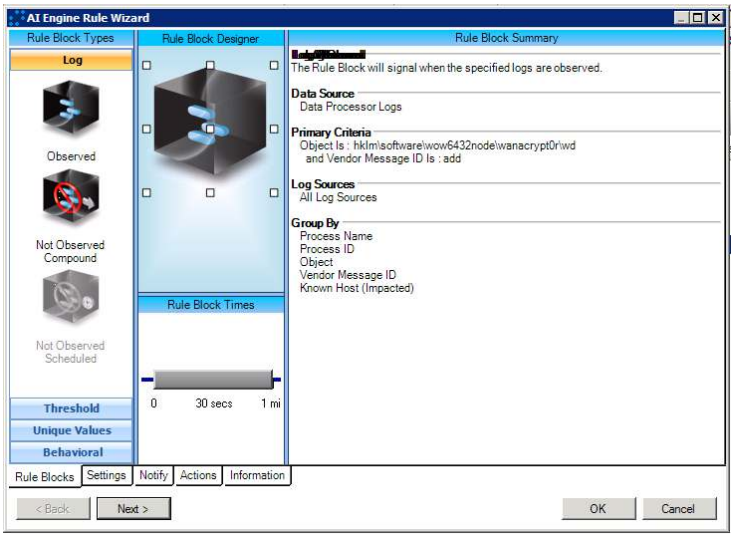
For further guidance, refer to the following Microsoft blog article that references an emergency patch that was issued for customers who are running unsupported operating systems.

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

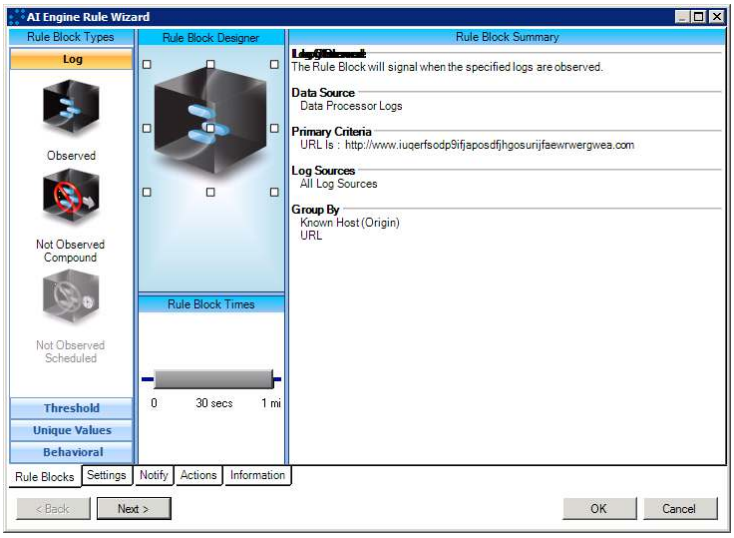
LogRhythm Signatures



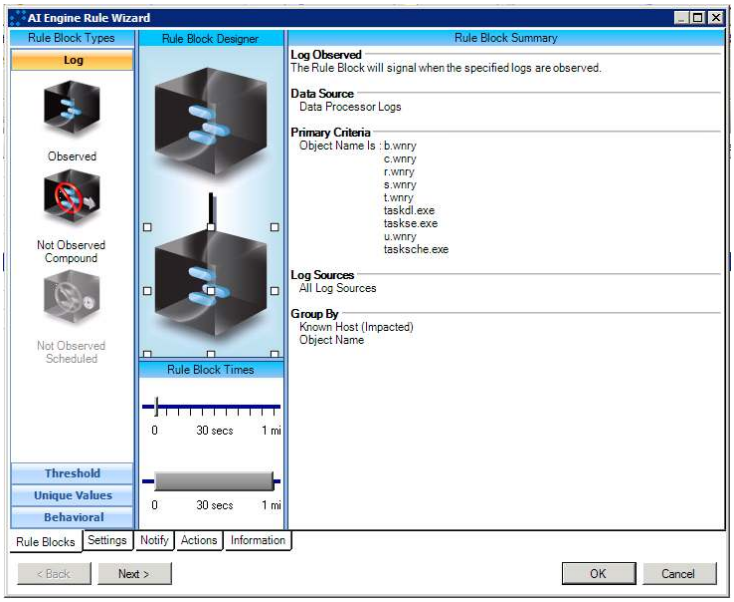
WannaCry_Command Arguments



WannaCry_RegistryKeyCreation



WannaCry_Initial Callout



WannaCry_Tor-EncryptorFile

Network Monitor Query Rules

The following signatures can identify the initial Wannacry dropper SMB exploit. These signatures may generate false positives in some network environments.

Application:SMB AND Version:1 AND CommandString:*transaction2_secondary*
Application:SMB AND Version:1 AND (Path:192.168.56.20 OR Path:172.16.99.5)

Indicators of Compromise

SHA256 Hash Values

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
0e5ece918132a2b1a190906e74becb8e4ced36eec9f9d1c70f5da72ac4c6b92a
9b3262b9faecb28da4637444f54c060c8d884c3e8cf676815e8ae5a72af48ed4
d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa
1465987e3c28369e337f00e59105dea06a3d34a94c2a290caed887e2fed785ac
402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c
e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b
97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6
4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
4870714e654ad4ca7b480b81195f29c56353c6f42d66754ad414c1bc1d25fbb9
bdc8f135484daf898c6d76a244e630a797652b0af1722712515ce844c66bf4af
71b25aeae6470f9ab93db1e80a500bf61282ae8dc505a8e3c781309e46037613
963caaac4a537ad1250fe77510906236261bc7b8ac3c72269d6c059cb5f8f71d

About LogRhythm

LogRhythm, a leader in Threat Lifecycle Management, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyberthreats. The company's patented award-winning platform unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration (SAO) and advanced security analytics. In addition to protecting customers from the risks associated with cyberthreats, LogRhythm provides compliance automation and assurance, and enhanced IT intelligence.

Among its many industry accolades, LogRhythm has been positioned as a Leader in Gartner's SIEM Magic Quadrant, received SC Labs' "Recommended" rating for SIEM and UTM for 2017 and won "Best SIEM" in SANS Institute's "Best of 2016 Awards."

LogRhythm® Labs

About LogRhythm Labs

The LogRhythm Labs team deliveres unparalleled security research, analytics, incident response and threat intelligence services to protect your organization from damaging cyber threats.

We empower you by combining actionable intelligence with advanced analytics so you can greatly reduce the time to detect and remediate against the risks that matter the most to you.

Contact us:

1-866-384-0713
info@logrhythm.com | www.logrhythm.com
Worldwide HQ, 4780 Pearl East Circle, Boulder CO, 80301

LogRhythm®
The Security Intelligence Company