



# MAMBA RANSOMWARE ANALYSIS

LogRhythm Labs

August 2017

# Table of Contents

- 3 Summary
- 3 Analysis
- 6 Base64 Encoded Strings
- 7 LogRhythm Signatures
- 10 Network Monitor Signatures



## Summary

In September of 2016, a strain of ransomware was discovered in the wild that performed full disk encryption. According to Kaspersky Lab researchers<sup>1</sup>, this ransomware strain, named “Mamba,” now appears to be recirculating, primarily in Brazil and Saudi Arabia. The ransomware includes a DiskCryptor tool capable of using strong encryption algorithms to make recovering the encrypted disk content next to impossible, unless the victim is able to obtain a decryption key from the ransom authors. The resurgence of this malware has prompted analysis efforts by Labs researchers to ensure users are prepared to protect their systems and help prevent infection of this malware variant in the future. In-depth analysis of this latest Mamba sample is presented below and signatures in support of detection are included at the end of this report.

## Analysis

The Mamba dropper sample analyzed has the following respective MD5 and SHA256 hashes, and will be referred to as “b9b60.exe” for the remainder of this report:

MD5: 79ed93df3bec7cd95ce60e6ee35f46a1

SHA256: b9b6045a45dd22fcdf2fc13d39eba46180d489cb4eb152c87568c2404aecac2f

Upon executing the dropper, Mamba creates the folders “C:\xampp\http”. This would appear to mimic the open source XAMPP application distribution<sup>2</sup>, which is a cross-platform package containing the web server Apache, database MariaDB, and the PHP and Perl programming languages. The directory mimicked by the malware is specifically the Apache web server component directory configured by XAMPP.

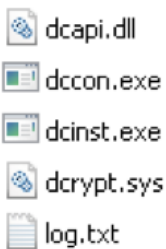


Table 1: Files Dropped in C:\xampp\http

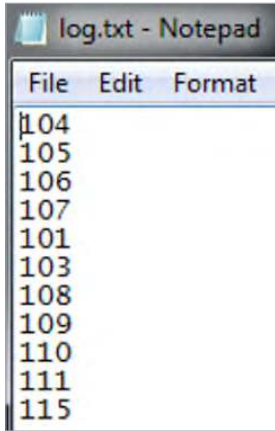
Filename	Description	MD5	SHA-256
dcapi.dll	Cryptor library	b4c9a8deb15e312aecaec27d5fbc898f	7fc78f3e1a6963185dac4af949fb76fd79b429148f9f61d429054e94f7a8ba32
dccon.exe	Console version of DiskCryptor	1a1222101c499eb15f5c91774583d24d	2dd5dd9aa62a9072753fdf82a2d4b386401c00f59755a755d68cb6bbb608203c
dcinst.exe	Cryptor installer support	88f25e2f08c90b3bbe253d0d64abd3e	9136ee4e2b73dd617d116fc28e6673931043f03e94a6ee4f0b57a29609f96749
dcrypt.sys	Cryptor driver	edb72f4a46c39452d1a5414f7d26454a	0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6
log.txt	Created by malware, logs codes indicating malware activity	1395dbadb21547be726872e3206d0e23	04f0e45b35a21d060d8d2324541739bc1c550ee0e6526b2685ae0b6bdd379447

Table 2: Description of Dropped Files

<sup>1</sup>Kaspersky Labs, “The return of Mamba ransomware,” <https://securelist.com/the-return-of-mamba-ransomware/79403/>

<sup>2</sup>XAMPP Apache Distribution, <https://www.apachefriends.org/index.html>

In the case of the log.txt file created by the malware, this appears to track the activity of the malware. While the code references are still being analyzed, the value “107” in the log indicates successful creation of the service used for persistence, called “DefragmentService”.



log.txt file contents

The malware contains the DiskCryptor cryptography tool<sup>3</sup> embedded as resources in the main malware binary as shown below. According to the DiskCryptor documentation, the tool supports AES, TwoFish and Serpent encryption algorithms. Analysis is still ongoing in order to determine the specific encryption algorithm used by Mamba.



Table 3: 32- and 64-bit DiskCryptor Binary Resources

<sup>3</sup>DiskCryptor Open Source Partition Encryption Solution, <https://diskcryptor.net/wiki/Downloads>

<sup>4</sup>Note that the DependOnService makes use of the Filter Manager by installing a mini filter driver which can be viewed when running the command “fltmc instances”:

Filter	Volume Name	Altitude	Instance Name	Frame	VIStatus
luafv	C:	135000	luafv	0	
dcrypt	C:	87150	dcrypt	0	
FileInfo	\Device\Mup	45000	FileInfo	0	
FileInfo	C:	45000	FileInfo	0	

<sup>5</sup>An ErrorControl value 0x3 as seen in dynamic analysis is unusual and requires further analysis to determine whether this is intentional behavior of the malware or a side effect of execution.

Note that further analysis and correlation of the dropped files and the publicly available versions is still underway. Although the hashes of the dropped files do not directly match those of the publicly available versions, static analysis suggests that the functionality is nearly identical. Although analysis of these files is ongoing, it is likely that the malware authors simply recompiled the available DiskCryptor source code for inclusion in Mamba.

After dropping the DiskCryptor files, Mamba additionally performs the following:

- Runs “C:\xampp\http\dcinst.exe -setup”
- **dcinst.exe** moves the cryptographic driver to %WinDir%\System32\drivers\dcrypt.sys
- Two services are created named “**dcrypt**” and “**DefragmentService**” with the following registry values:

HKLM\System\CurrentControlSet\services\dcrypt	
Name	Data
DependOnService	FltMgr <sup>4</sup>
DisplayName	DiskCryptor driver
Group	Filter
ImagePath	system32\drivers\dcrypt.sys
ErrorControl	0x3 (Record the current startup as a failure) <sup>5</sup>
Start	0x0 (Boot)
Type	0x1 (Kernel-mode driver)

HKLM\System\CurrentControlSet\services\DefragmentService			
Name	Data		
DisplayName	Defragment Service		
ImagePath	<path to malware exe> <password> <2 <sup>nd</sup> parameter> <sup>6</sup>		
ErrorControl	0x0 (Ignore)		
Start	0x2 (Automatic)		
Type	0x10 (16: A Win32 program that runs in a process by itself.)		
FailureActions	Value <sup>7</sup>	Data	Description
	ResetPeriod	0x78	Reset failure count to zero after 120 (0x78) seconds if there have been no failures
	RebootMsg	0x1	Unknown value
	Command	0x0	Command line of the process is unchanged
	Actions	0x2	Number of elements in SC Actions array below
	SC Action ptr	0x14	Pointer to SC Action array
	SC Action 1	0x1 0x3E8	Restart the service after 1000 (0x3E8) ms
	SC Action 2	0x1 0x3E8	Restart the service after 1000 (0x3E8) ms

- If the “DefragmentService” service is successfully created, the malware forces a reboot of the infected host, ensuring persistence for the malware
- After reboot, the malware runs the command-line encryption tool dccon.exe to encrypt the file system
  - This task runs under the original malware process name registered as a service in the above step

While the encryption process is running, entering the command “dccon.exe -info pt0” from a command-prompt will allow one to view the encryption progress, encryption type, and other details:

```
Device:          \Device\HarddiskVolume1
SymLink:         \\?\Volume{32a3a004-feb3-11e6-b3af-806e6f6e6963}
Mount point:     C:
Capacity:        499 GB
Status:          mounted, boot, system
Cipher:          AES
Encryption mode: XTS
Pkcs5.2 prf:     HMAC-SHA-512
Encrypted portion: 4.579%
```

Figure 1: Sample output of “dccon.exe -info pt0”

Once the encryption process completes, and after a further reboot, the victim is presented with the following ransom note, which requests that the user email one of two email addresses with an ID number, presumably to retrieve the decryption key. Note that there is no indication of what the actual ransom fee is.

```
Your Data Encrypted, Contact For Key( mcript2017@yandex.com OR citrix2234@protonmail.com ) Your ID : 721 ,Enter Key:_
```

Figure 2: Ransom Message Following Successful Encryption

<sup>6</sup> The first parameter is a password for the encryption and can be any value; the original value is unknown. The second parameter is required, and (reportedly) expected to be “/accepteula” (due to the typical execution via the Sysinternals tool psexec), but the malware will execute as long as any 2 arguments are passed in.

<sup>7</sup> This value is binary data in the format of a SERVICE\_FAILURE\_ACTIONS structure as documented in [https://msdn.microsoft.com/en-ca/library/windows/desktop/ms685939\(v=vs.85\).aspx](https://msdn.microsoft.com/en-ca/library/windows/desktop/ms685939(v=vs.85).aspx)

## Base64 Encoded Strings

The analyzed Mamba sample utilizes Base64 encoding in order to obfuscate strings in the binary that reveal the malware's functionality. Listed below are the decoded strings extracted from the binary. Note that some of the strings listed below are commands that were not observed to be used during execution.

Encoded Base64 String	Decoded Base64 String
V293NjREaXNhYmxlV293NjRGc1JlZGlyZWNOaW9u	Wow64DisableWow64FsRedirection
S2VybmVsMzluZGxs	Kernel32.dll
b3Blbg==	open
ICYgc2h1dGRvd24gL2YgL3lgL3QgMA==	& shutdown /f /r /t 0
ICYgdGFza2tpbGwgL2ltIE1vdW50LmV4ZSAmIERlbCAiQzpcVXNlcnNcQUJDRFxB3VudC5leGUiICYgRGVslCJD0lxVc2Vyc1xBQkNEXG5ldHBhc3MudHh0IiAgJiBEZWwgIkM6XFVzZXJzXEFQC0RcbmV0dXNlLnR4dClgICYgRGVslCJD0lxVc2Vyc1xBQkNEXG5ldHBhc3MuZXhliAmIG5ldCB1c2VyIC9kZWwgblXl0aGJlc3RlcnM=	& taskkill /im Mount.exe & Del "C:\Users\ABCD\Mount.exe" & Del "C:\Users\ABCD\netpass.txt" & Del "C:\Users\ABCD\netuse.txt" & Del "C:\Users\ABCD\netpass.exe" & net user /del mythbusters
L0MgcGluZyAxLjEuMS4xIC1uIDEGlXcGZAwMCA+IE51bCAmIHNjIGRlbgVOZSBEZWZyYWdtZW50U2VydmliZSAmIERlbCAi	/C ping 1.1.1.1 -n 1 -w 3000 > Nul & sc delete DefragmentService & Del "-boot -setmbr hd0
LWJvb3QgLXNldG1iciBoZDA=	-boot -setmbr hd0
LWVuY3J5cHQgcHQ0IC1wIA==	-encrypt pt4 -p
LWVuY3J5cHQgcHQ1IC1wIA==	-encrypt pt5 -p
LWVuY3J5cHQgcHQ2IC1wIA==	-encrypt pt6 -p
LWVuY3J5cHQgcHQ3IC1wIA==	-encrypt pt7 -p
LWVuY3J5cHQgcHQ4IC1wIA==	-encrypt pt8 -p
LWVuY3J5cHQgcHQ5IC1wIA==	-encrypt pt9 -p
LWVuY3J5cHQgcHQwIC1wIA==	-encrypt pt0 -p
LWVuY3J5cHQgcHQxIC1wIA==	-encrypt pt1 -p
LWVuY3J5cHQgcHQyIC1wIA==	-encrypt pt2 -p
LWVuY3J5cHQgcHQzIC1wIA==	-encrypt pt3 -p
LXNldHVw	-setup32dcapi.dll
MzJkY2FwaS5kbGw=	32dcapi.dll
MzJkY2luc3QuZXhl	32dcinst.exe
MzJkY2Nvbi5leGU=	32dccon.exe
MzJkY3J5cHQuc3lz	32dcrypt.sys
NjRkY2FwaS5kbGw=	64dcapi.dll
NjRkY2luc3QuZXhl	64dcinst.exe
NjRkY2Nvbi5leGU=	64dccon.exe
NjRkY3J5cHQuc3lz	64dcrypt.sys
QzpcVXNlcnNcQUJDRFxuZXRwYXNzLnR4dA==	C:\Users\ABCD\netpass.txt
RGVmcmFnbWVudFNlcnZpY2U=	DefragmentService
XGRjaW5zdC5leGU=	\dcinst.exe
XGRjY29uLmV4ZQ==	\dccon.exe
Y2lk	cmd
ZGNhcGkuZGxs	dcapi.dll
ZGNjb24uZXhl	dccon.exe
ZGNpbmN0LmV4ZQ==	dcinst.exe
ZGNyeXBOLnN5cw==	dcrypt.sys

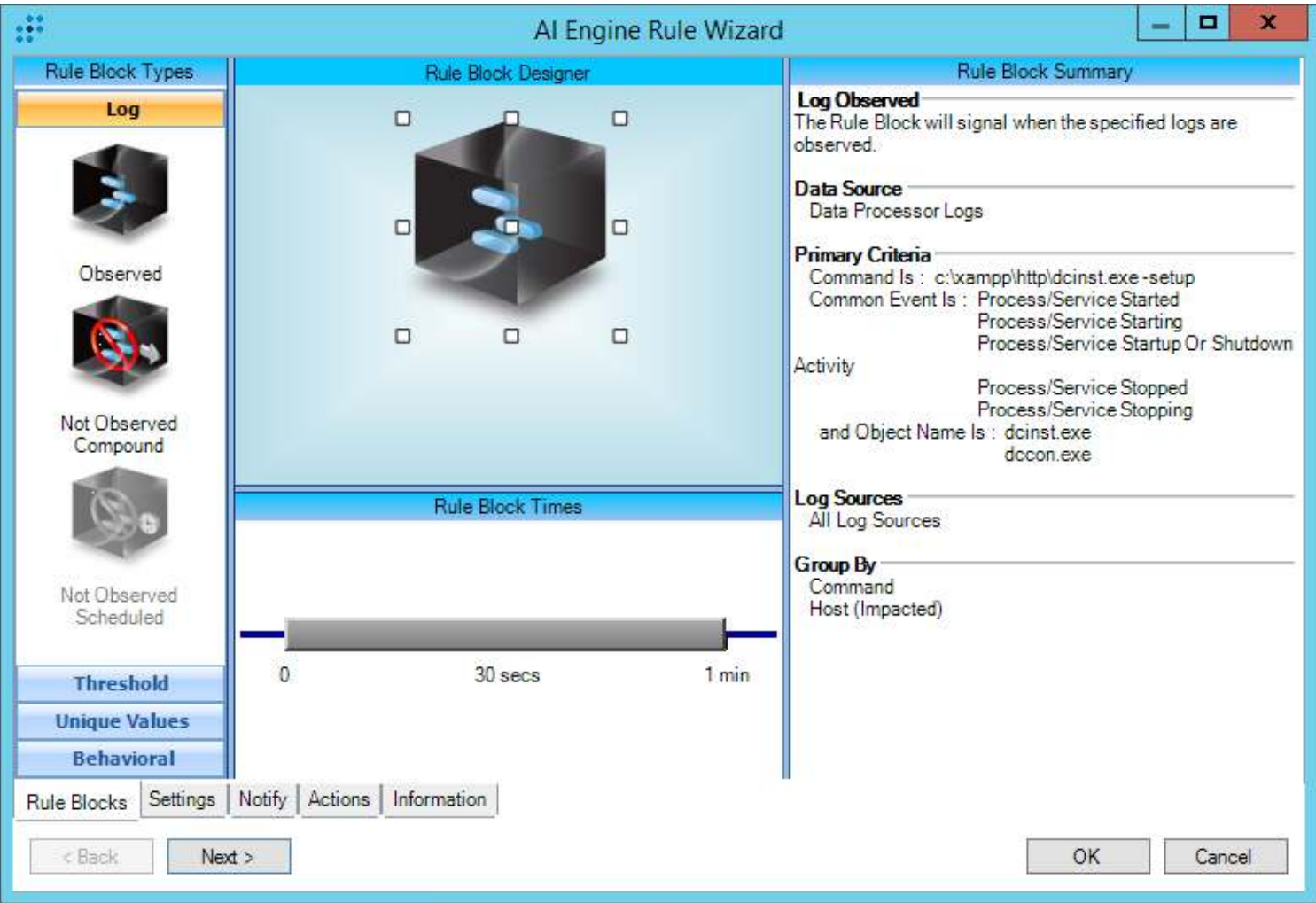


Network Artifacts

This variant of Mamba does not exhibit any notable network functionality. Unlike the recent ransomware outbreaks of WanaCry and NotPetya, this variant of Mamba does not contain any inherent exploitation or spreading functionality. The malware is executed solely on the infected host and will not self-replicate.

LogRhythm Signatures

There are four LogRhythm AI Engine rules that have been created to detect some of the main indicators that we observed in our internal lab environment.



Labs Mod - Mamba - Command - DiskCryptor Installation


Rule Block Types	Rule Block Designer	Rule Block Summary
<b>Log</b>  Observed  Not Observed Compound  Not Observed Scheduled <b>Threshold</b> <b>Unique Values</b> <b>Behavioral</b>	 <b>Rule Block Times</b> 	<b>Log Observed</b> The Rule Block will signal when the specified logs are observed. <hr/> <b>Data Source</b> Data Processor Logs <hr/> <b>Primary Criteria</b> Object Is : c:\xampp\htdocs\dcrpt.sys and Object Name Is : dcrpt.sys and Subject Is : c:\windows\system32\drivers\dcrptsys and Process Name Is : dllhost.exe Object Is : c:\windows\system32\drivers\dcrptsys and Object Name Is : dcrpt.sys and Command Is : add <hr/> <b>Log Sources</b> All Log Sources <hr/> <b>Group By</b> Host (Impacted) Object Object Name

Rule Blocks   Settings   Notify   Actions   Information




Rule Block Types


Log



Observed



Not Observed Compound



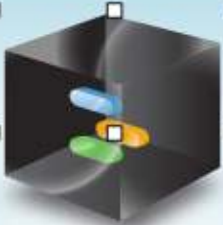
Not Observed Scheduled

Threshold


Unique Values

Behavioral

Rule Block Designer



Rule Block Times



Rule Block Summary

Unique Values Observed

The Rule Block will signal if 3 or more unique occurrences of Object Name are observed within 1 minute.

Data Source

Data Processor Logs

Primary Criteria

Object Name Is : c:\xampp\htdocs\dcapi.dll  
c:\xampp\htdocs\dccon.exe  
c:\xampp\htdocs\dcinst.exe  
c:\xampp\htdocs\dcrypt.sys  
c:\xampp\htdocs\log.txt

Log Sources

All Log Sources

Group By

Host (Impacted)

Unique Values

Object Name >= 3

Rule Blocks

Settings

Notify

Actions

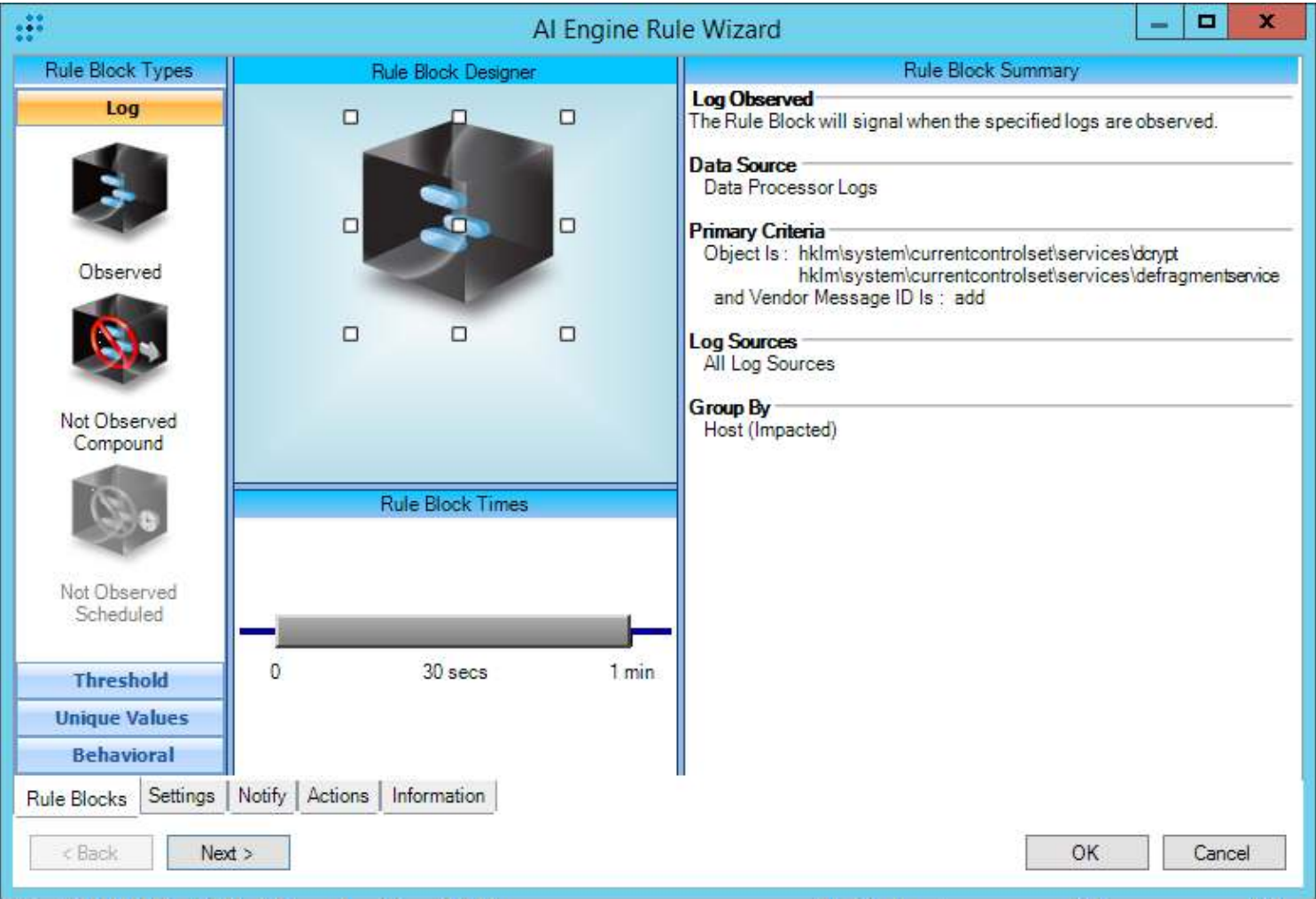
Information

< Back

Next >

OK

Cancel



Labs Mod - Mamba - Registry Key Creation

Network Monitor Signatures

As there does not appear to be any network artifacts produced on the infected host, there are currently no Lucene Searches or DPA rules for Network Monitor at this time.

### 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."



### About LogRhythm Labs

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

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](mailto:info@logrhythm.com) | [www.logrhythm.com](http://www.logrhythm.com)

Worldwide HQ, 4780 Pearl East Circle, Boulder CO, 80301

 **LogRhythm®**  
The Security Intelligence Company