MVISION Insights: Wastedlocker Ransomware

Technical Articles ID: KB93302
Last Modified: 8/28/2020

Environment

IMPORTANT: This Knowledge Base article discusses a specific threat that is being automatically tracked by MVISION Insights technology. The co
intended for use by MVISION Insights users, but is provided for general knowledge to all customers. Contact us for more information about MVISI
Insights.

Summary

Description of Campaign
The Evil Corp eCrime group, also known as Indrik Spider, released a new ransomware family known as WastedLocker which uses AES and RSA
encryption. A customized string is appended to encrypted files consisting of the company's name and the word "wasted". A ransom note is droppe
each infected file and states the victim must contact the threat actor at one of two email addresses. The ransom demand can reach into the millio
dollars. The group behind WastedLocker is known to also be the same group that has distributed malware in the past, including ransomware, ban
trojans, and botnets.

How to use this article:

1. If a Threat Hunting table has been created, use the rules contained to search for malware related to this campaign.
2. Review the product detection table and confirm that your environment is at least on the specified content version.
   To download the latest content versions, go to the Security Updates page.
3. Scroll down and review the "Product Countermeasures" section of this article. Consider implementing them if they are not already in place.
4. Review KB91836 - Countermeasures for entry vector threats.
5. Review KB87843 - Dynamic Application Containment rules and best practices.
6. Review KB82925 - Identify what rule corresponds to an Adaptive Threat Protection and Threat Intelligence Exchange event.

Campaign IOC

Type	Value
SHA256	BCDAC1A2B67E2B47F8129814DCA3BCF7D55404757EB09F1C3103F57DA3153EC8
SHA256	AA05E7A187DDEC2E11FC1C9EAFE61408D085B0AB6CD12CAEAF531C9DCA129772
SHA256	85F391ECD480711401F6DA2F371156F995DD5CFF7580F37791E79E62B91FD9EB
SHA256	5CD04805F9753CA08B82E88C27BF5426D1D356BB26B281885573051048911367
SHA256	817704ED2F654929623D9D3E4B71CE0082EF4EADB3FE2D80C726E874DC6952A3
SHA256	887AAC61771AF200F7E58BF0D02CB96D9BEFA11DEDA4E448F0A700CCB186CE9D
SHA256	8897DB876553F942B2EB4005F8475A232BAFB82A50CA7761A621842E894A3D80
SHA256	ED0632ACB266A4EC3F51DD803C8025BCCD654E53C64EB613E203C590897079B3
SHA256	E3BF41DE3A7EDF556D43B6196652AA036E48A602BB3F7C98AF9DAE992222A8EB
SHA256	905EA119AD8D3E54CD228C458A1B5681ABC1F35DF782977A23812EC4EFA0288A
SHA256	7A45A4AE68992E5BE784B4A6DA7ACD98DC28281FE238F22C1F7C1D85A90D144A
SHA256	AB007094AFEC534A2AA64436F214866014A664E7399AEAF361790EDE5EEC6B56
SHA256	EF7A9166C63D90CD5A4C5C58CB458DA4C967A2BAAB2AD433DE0AA20DFBF568F7
SHA256	AE255679F487E2E9075FFD5E8C7836DD425229C1E3BD40CFC46FBBCECEEC7CF4
SHA256	4D7E4660C8E71D4D663DAC8EA2B8CDE6E07277B2839BEDA6AD88EB66F3F5A71B
SHA256	D054E9223A2665B1746727D7BF9B008181C2D60C6A20B27490E4ADB151560823
SHA256	C9473B2E24732DE1C123C48DA231E5497E0EA5324A62C9B80BDD8DADFDB0FE3A
SHA256	9744B5F5D07149C5619D7FEC67622B4E43BF3B28A803C2AB4121BE4080E2B165
SHA256	80FED3BC3510201687ED4DD3F6F56D5F8D2B14B87B065787BD97192A44B71B94

SHA256	9A4A06FECA395FCD3C11ADB8AD6FE21C8BA63A56ABC7B1C95F0ADEDC4EAA8D35
SHA256	37A30621364D3083424B24B0255FC8F5752D88C381600D840574E551C284FB6E
SHA256	6D35B01DBE014C6EFC18D587C2BE5E12617E1681CC670BA5C49FE7EAD9DE780E

Minimum Content Versions:

Content Type	Version
V2 DAT (VirusScan Enterprise)	9713
V3 DAT (Endpoint Security)	4165

Detection Summary

IOC	Scanner	Detection
BCDAC1A2B67E2B47F8129814DCA3BCF7D55404757EB09F1C3103F57DA3153EC8	AVEngine V2	Ransom-Wasted t
AVEngine V3	Ransom-Wasted trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect-EC!0ED2CA539A01	
RP Dynamic	-	

IOC	Scanner	Detection
AA05E7A187DDEC2E11FC1C9EAFE61408D085B0AB6CD12CAEAF531C9DCA129772	AVEngine V2	Ransom-Wasted
AVEngine V3	Ransom-Wasted trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect-EC!13E623CDFB75	
RP Dynamic	-	

IOC	Scanner	Detection
85F391ECD480711401F6DA2F371156F995DD5CFF7580F37791E79E62B91FD9EB	AVEngine V2	Trojan-Cobalt troja
AVEngine V3	Trojan-Cobalt trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect-PEE!3208A14C9BAD	
RP Dynamic	-	

IOC	Scanner	Detection
5CD04805F9753CA08B82E88C27BF5426D1D356BB26B281885573051048911367	AVEngine V2	Ransom-Wasted trojan
AVEngine V3	Ransom-Wasted trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect.bx!572FEA5F025D	
RP Dynamic	-	

IOC	Scanner	Detection
817704ED2F654929623D9D3E4B71CE0082EF4EADB3FE2D80C726E874DC6952A3	AVEngine V2	Ransom-Wasted
AVEngine V3	Ransom-Wasted	
JTI (ATP Rules)	ATP/Suspect!0d1241967ee4	

RP Static	-
RP Dynamic	-

IOC	Scanner	Detection
887AAC61771AF200F7E58BF0D02CB96D9BEFA11DEDA4E448F0A700CCB186CE9D	AVEngine V2	Ransom-Wasted t
AVEngine V3	Ransom-Wasted trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect-EC!6B20EF8FB494	
RP Dynamic	-	

IOC	Scanner	Detection
8897DB876553F942B2EB4005F8475A232BAFB82A50CA7761A621842E894A3D80	AVEngine V2	Ransom-Wasted troj
AVEngine V3	Ransom-Wasted trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect-EC!ECB00E9A61F9	
RP Dynamic	-	

IOC	Scanner	Detection
ED0632ACB266A4EC3F51DD803C8025BCCD654E53C64EB613E203C590897079B3	AVEngine V2	Trojan-Cobalt troj
AVEngine V3	Trojan-Cobalt trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect-SS!EDBF07EACA4F	
RP Dynamic	-	

IOC	Scanner	Detection
E3BF41DE3A7EDF556D43B6196652AA036E48A602BB3F7C98AF9DAE992222A8EB	AVEngine V2	Ransom-Wasted tro
AVEngine V3	Ransom-Wasted trojan	
JTI (ATP Rules)	-	
RP Static	Real Protect.bx!F67EA8E471E8	
RP Dynamic	-	

IOC	Scanner	Detection
905EA119AD8D3E54CD228C458A1B5681ABC1F35DF782977A23812EC4EFA0288A	AVEngine V2	Packed-GCI!2CC4534B0
AVEngine V3	Packed-GCI!2CC4534B0DD0	
JTI (ATP Rules)	JTI/Suspect.196612!2cc4534b0dd0	
RP Static	Real Protect-EC!2CC4534B0DD0	
RP Dynamic	-	

IOC	Scanner	Detection
7A45A4AE68992E5BE784B4A6DA7ACD98DC28281FE238F22C1F7C1D85A90D144A	AVEngine V2	Ransom-Wasted!2000DE399
AVEngine V3	Ransom-Wasted!2000DE399F4C	
JTI (ATP Rules)	-	

RP Static	Real Protect-PEE!2000DE399F4C
RP Dynamic	-

IOC	Scanner	Detection
AB007094AFEC534A2AA64436F214866014A664E7399AEAF361790EDE5EEC6B56	AVEngine V2	Ransom-Wasted!33B80A574C
AVEngine V3	Ransom-Wasted!33B80A574C64	
JTI (ATP Rules)	-	
RP Static	Real Protect-EC!33B80A574C64	
RP Dynamic	-	

IOC	Scanner	Detection
EF7A9166C63D90CD5A4C5C58CB458DA4C967A2BAAB2AD433DE0AA20DFBF568F7	AVEngine V2	Ransom-Wasted!47EBBBD8
AVEngine V3	Ransom-Wasted!47EBBBD8CA06	
JTI (ATP Rules)	-	
RP Static	Real Protect-PEE!47EBBBD8CA06	
RP Dynamic	-	

IOC	Scanner	Detection
AE255679F487E2E9075FFD5E8C7836DD425229C1E3BD40CFC46FBBCECEEC7CF4	AVEngine V2	GenericRXAA-AA!813B274EC331
AVEngine V3	GenericRXAA-AA!813B274EC331	
JTI (ATP Rules)	-	
RP Static	Real Protect-PEE!813B274EC331	
RP Dynamic	-	

IOC	Scanner	Detection
4D7E4660C8E71D4D663DAC8EA2B8CDE6E07277B2839BEDA6AD88EB66F3F5A71B	AVEngine V2	Ransom-Wasted!8FE65F631
AVEngine V3	Ransom-Wasted!8FE65F63196D	
JTI (ATP Rules)	-	
RP Static	Real Protect-PEE!8FE65F63196D	
RP Dynamic	-	

IOC	Scanner	Detection
D054E9223A2665B1746727D7BF9B008181C2D60C6A20B27490E4ADB151560823	AVEngine V2	Ransom-Wasted!9259850958
AVEngine V3	Ransom-Wasted!9259850958FF	
JTI (ATP Rules)	-	

RP Static	Real Protect-PEE!9259850958FF
RP Dynamic	-

IOC	Scanner	Detection
C9473B2E24732DE1C123C48DA231E5497E0EA5324A62C9B80BDD8DADFDB0FE3A	AVEngine V2	Ransom-Wasted!A091197C7
AVEngine V3	Ransom-Wasted!A091197C76CA	
JTI (ATP Rules)	-	
RP Static	Real Protect-PEE!A091197C76CA	
RP Dynamic	-	

IOC	Scanner	Detection
9744B5F5D07149C5619D7FEC67622B4E43BF3B28A803C2AB4121BE4080E2B165	AVEngine V2	Ransom-Wasted
AVEngine V3	Ransom-Wasted	
JTI (ATP Rules)	-	
RP Static	Real Protect-PEE!D47DE19B52F9	
RP Dynamic	-	

IOC	Scanner	Detection
80FED3BC3510201687ED4DD3F6F56D5F8D2B14B87B065787BD97192A44B71B94	AVEngine V2	Ransom-Wasted!1DE62A9B8
AVEngine V3	Ransom-Wasted!1DE62A9B82F4	
JTI (ATP Rules)	-	
RP Static	Real Protect-PEE!E1216B076CA5	
RP Dynamic	-	

IOC	Scanner	Detection
9A4A06FECA395FCD3C11ADB8AD6FE21C8BA63A56ABC7B1C95F0ADEDC4EAA8D35	AVEngine V2	Ransom-Wasted!1CD3
AVEngine V3	Ransom-Wasted!1CD33F096A49	
JTI (ATP Rules)	JTI/Suspect.196612!eb1fd07eb54f	
RP Static	Real Protect-PEE!EB1FD07EB54F	
RP Dynamic	-	

IOC	Scanner	Detection
37A30621364D3083424B24B0255FC8F5752D88C381600D840574E551C284FB6E	AVEngine V2	Ransom-Wasted!6D9AD19726
AVEngine V3	Ransom-Wasted!6D9AD19726C7	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
6D35B01DBE014C6EFC18D587C2BE5E12617E1681CC670BA5C49FE7EAD9DE780E	AVEngine V2	Ransom-Wasted!9B5F5E7D1
AVEngine V3	Ransom-Wasted!9B5F5E7D14BD	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

Minimum set of Manual Rules to improve protection to block this campaign

IMPORTANT: Always follow best practices when you enable new rules and signatures.

When you implement new rules or signatures, always set them to **Report** mode first and check the alerts generated. Resolve any issues that aris set the rules to **Block**. This step mitigates against triggering false positives and allows you to refine your configuration.

For more information, see KB87843 - List of and best practices for Endpoint Security Dynamic Application Containment rules.
Endpoint Security - Advanced Threat Protection:
Rule ID: 4 Use GTI file reputation to identify trusted or malicious files
Endpoint Security - Access Protection Custom Rules:
Rule: 1
Executables (Include):
*
Subrules:
Subrule Type: Files
Operations:
create
Targets (Include):
?:\users*\appdata\roaming*:bin
Rule: 2
Executables (Include):
*
Subrules:
Subrule Type: Files
Operations:
create
Targets (Include):
*.garminwasted
*.garminwasted_info

VirusScan Enterprise - Access Protection Custom Rules:

Rule: 1
Rule Type: File
Process to include: *
File or folder name to block: *\users*\appdata\roaming*:bin
File actions to prevent: Create

Rule: 2
Rule Type: File
Process to include: *
File or folder name to block: *.garminwasted
File actions to prevent: Create

Rule: 3
Rule Type: File
Process to include: *
File or folder name to block: *.garminwasted_info
File actions to prevent: Create

Aggressive set of Manual Rules to improve protection to block this campaign

IMPORTANT: Always follow best practices when you enable new rules and signatures.

When you implement new rules or signatures, always set them to **Report** mode first and check the alerts generated. Resolve any issues that aris set the rules to **Block**. This step mitigates against triggering false positives and allows you to refine your configuration.

For more information, see KB87843 - List of and best practices for Endpoint Security Dynamic Application Containment rules.
Virusscan Enterprise - Access Protection Rules:
Prevent programs registering to autorun
Prevent programs registering as a service

Host Intrusion Prevention:

Rule ID: 6053 Accessing other users home directory
Rule ID: 990 New Startup Folder Program Creation
Rule ID: 1148 CMD Tool Access by a Network Aware Application
Rule ID: 1020 Windows Agent Shielding - File Access
Rule ID: 412 Double File Extension Execution
Rule ID: 6011 Generic Application Invocation Protection
Rule ID: 2806 Attempt to create a hardlink to a file
Rule ID: 6010 Generic Application Hooking Protection
Rule ID: 344 New Startup Program Creation
Rule ID: 2265 Delay Delete File Protection

Endpoint Security - Dynamic Application Containment:
Modifying the Services registry location

Endpoint Security - Exploit Prevention:
Rule ID: 344 New Startup Program Creation