Trellix Insights: SmokeLoader Exploits Old Vulnerabilities to Drop zgRAT

kcm.trellix.com/corporate/index

Get support for FireEye products →

Technical Articles ID: KB96190
Last Modified: 2022-11-17 08:46:51 Etc/GMT

Environment

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

Summary

Description of Campaign
An attack campaign was discovered using SmokeLoader to deliver zgRAT through phishing emails with malicious attachments. The operation used two Microsoft Office vulnerabilities, CVE-2017-0199 and CVE-2017-11882, to gain access, elevate privileges, and download the malware to the infected device. The attackers used a Gzip archive that pretended to be an image file and a Microsoft .NET executable that described itself as an archive file.

Our Threat Research team gathers and analyzes information from multiple open and closed sources before disseminating intelligence reports. This campaign was researched by Fortinet and shared publicly.

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.

Threat Hunting

YARA

```
rule MALWARE_Win_zgRAT {
meta:
author = "ditekSHen"
description = "Detects zgRAT"
strings:
$s1 = "file:///" fullword wide
$s2 = "{11111-22222-10009-11112}" fullword wide
$s3 = "{11111-22222-50001-00000}" fullword wide
$s4 = "get_Module" fullword ascii
$s5 = "Reverse" fullword ascii
$s6 = "BlockCopy" fullword ascii
$s7 = "ReadByte" fullword ascii
$s8 = { 4c 00 6f 00 63 00 61 00 74 00 69 00 6f 00 6e 00
00 0b 46 00 69 00 6e 00 64 00 20 00 00 13 52 00
65 00 73 00 6f 00 75 00 72 00 63 00 65 00 41 00
00 11 56 00 69 00 72 00 74 00 75 00 61 00 6c 00
20 00 00 0b 41 00 6c 00 6c 00 6f 00 63 00 00 0d
57 00 72 00 69 00 74 00 65 00 20 00 00 11 50 00
72 00 6f 00 63 00 65 00 73 00 73 00 20 00 00 0d
4d 00 65 00 6d 00 6f 00 72 00 79 00 00 0f 50 00
72 00 6f 00 74 00 65 00 63 00 74 00 00 0b 4f 00
70 00 65 00 6e 00 20 00 00 0f 50 00 72 00 6f 00
63 00 65 00 73 00 73 00 00 0d 43 00 6c 00 6f 00
73 00 65 00 20 00 00 0d 48 00 61 00 6e 00 64 00
6c 00 65 00 00 0f 6b 00 65 00 72 00 6e 00 65 00
6c 00 20 00 00 0d 33 00 32 00 2e 00 64 00 6c 00
6c }
condition:
uint16(0) == 0x5a4d and all of them
}
```

This Knowledge Base article discusses a specific threat that's being tracked. The list of IOCs will change over time; check Trellix Insights for the latest IOCs. **Campaign IOC**

Type	Value
SHA256	4E4E32F6259B82E6B932AB81172C22560EC2AC46E85543D4851637A63EAACE3E
SHA256	104F88876B4D7C963D47AFA63CFBB516D20E1CF9858D739F9C4023142B223FE2
SHA256	3223AE2C88753CE7268FA02213B76BDAF690AC37EC411EA8B7925C3B31E8822F
SHA256	EEF3295BADA101787AE4F1EBC92E17FC2C6CD8C39389A745C45943A019637CA1
SHA256	A1F59EBE9E8311267D831DA649A8DF44A3D747E9CF75E64A259B2FD917D2F587
DOMAIN	sorathlions.com
DOMAIN	dhemgldxkv.com
DOMAIN	afrocalite.com
URL	sorathlions.com/wp-content/Vymxn_Zfbgctbp.jpg

Minimum Content Versions

Content Type	Version
V2 DAT (VirusScan Enterprise)	10383
V3 DAT (Endpoint Security)	4835

Detection Summary

IOC	Scanner	Detection
4E4E32F6259B82E6B932AB81172C22560EC2AC46E85543D4851637A63EAACE3E	AVEngine V2	GenericRXTL-CU!5A1BB5D7F55F
AVEngine V3	GenericRXTL-CU!5A1BB5D7F55F	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
104F88876B4D7C963D47AFA63CFBB516D20E1CF9858D739F9C4023142B223FE2	AVEngine V2	GenericRXTL-CU!5A1BB5D7F55F
AVEngine V3	GenericRXTL-CU!5A1BB5D7F55F	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
3223AE2C88753CE7268FA02213B76BDAF690AC37EC411EA8B7925C3B31E8822F	AVEngine V2	Generic downloader.h
AVEngine V3	Generic downloader.h	

JTI (ATP Rules)	-
RP Static	-
RP Dynamic	-

IOC	Scanner	Detection
EEF3295BADA101787AE4F1EBC92E17FC2C6CD8C39389A745C45943A019637CA1	AVEngine V2	Exploit-GBW!132B8725CDEA
AVEngine V3	Exploit-GBW!132B8725CDEA	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	

IOC	Scanner	Detection
A1F59EBE9E8311267D831DA649A8DF44A3D747E9CF75E64A259B2FD917D2F587	AVEngine V2	Exploit-FYV!80F776694A0B
AVEngine V3	Exploit-FYV!80F776694A0B	
JTI (ATP Rules)	-	
RP Static	-	
RP Dynamic	-	