OSINT - Mitigating and eliminating info-stealing Qakbot and Emotet in corporate networks

General information

UUID	5a0ac036-6fbc-4855-83af-422b950d210f
Date	2017-11-06
Owner org	None
Threat level	3
Analysis	2
Info	OSINT - Mitigating and eliminating info-stealing Qakbot and Emotet in corporate networks
Event date	2017-11-20 13:25:52
Published	No
Creator Org	CIRCL
# Attributes	48
Tags	type:OSINT tlp:white osint:source-type="blog-post" misp-galaxy:tool="Emotet" misp-galaxy:banker="Qakbot"

Attributes

Attribute #0

UUID	5a0ac04b-331c-457e-9154-4535950d210f
Category	External analysis
Type	link
Value	https://blogs.technet.microsoft.com/mmpc/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/
Tags	osint:source-type="blog-post"

Attribute #1

UUID	5a0ac07e-7154-4727-9128-4b2b950d210f
Category	External analysis
Type	comment
Value	The threat to information is greater than ever, with data breaches, phishing attacks, and other forms of information theft like point-of-sale malware and ATM hacks becoming all too common in today's threat landscape. Information-stealing trojans are in the same category of threats that deliver a steady stream of risk to data and can lead to significant financial loss. Qakbot and Emotet are information stealers that have been showing renewed activity in recent months. These malware families are technically different, but they share many similarities in behavior. They both have the ultimate goal of stealing online banking credentials that malware operators can then use to steal money from online banking accounts. They can also steal other sensitive information using techniques like keylogging.
Tags	No tags

Attribute #2

UUID	5a0ac277-6480-4635-a01f-4b80950d210f
Category	Payload delivery
Comment	Qakbot malware
Type	sha256
Value	da00823090dae3dae452ddc8a4c2a3c087389b4aacf1f0c12d13c83c9fcaef9c
Tags	No tags

Attribute #3

UUID	5a0ac277-b4a0-490f-8e6a-4941950d210f
Category	Payload delivery
Comment	Qakbot malware
Type	sha256
Value	ca2d536b91b15e7fc44ec93bbed1f0f46ae65c723b8a4823253a2a91b8241f9a
Tags	No tags

Attribute #4

UUID	5a0ac405-e138-4948-8fd4-4827950d210f
Category	Payload delivery
Type	filename
Value	%APPDATA%\Microsoft\Cexpalgxx\Cexpalgxx.exe
Tags	No tags

Attribute #5

UUID	5a0ac405-1734-4d67-9c55-4422950d210f
Category	Payload delivery
Type	filename
Value	%APPDATA%\Microsoft\Cexpalgxx\Cexpalgxx32.dll
Tags	No tags

Attribute #6

UUID	5a0ac48c-b1fc-4778-9481-41b5950d210f
Category	Persistence mechanism
Type	regkey
Value	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Tags	No tags

Attribute #7

UUID	5a0ac4d2-bfa0-4123-a4c6-46e3950d210f
Category	Network activity
Type	ip-dst
Value	104.236.252.178
Tags	No tags

Attribute #8

UUID	5a0ac4d2-1274-4dff-b646-43f4950d210f
Category	Network activity
Type	ip-dst
Value	162.243.159.58
Tags	No tags

Attribute #9

UUID	5a0ac4d2-8568-4190-8a0b-489e950d210f
Category	Network activity
Type	ip-dst
Value	45.33.55.157
Tags	No tags

Attribute #10

UUID	5a0ac4d2-74d4-41c3-b9aa-4102950d210f
Category	Network activity
Type	ip-dst
Value	77.244.245.37
Tags	No tags

Attribute #11

UUID	5a0ac4d2-2050-407e-b273-4948950d210f
Category	Network activity
Type	ip-dst
Value	192.81.212.79
Tags	No tags

Attribute #12

UUID	5a0ac4d2-2ae4-4411-818f-4932950d210f
Category	Network activity
Type	ip-dst
Value	173.212.192.45
Tags	No tags

Attribute #13

UUID	5a0ac4d2-15f0-4c1f-a22e-4a3a950d210f
Category	Network activity
Type	ip-dst
Value	103.16.131.20
Tags	No tags

Attribute #14

UUID	5a0ac4d2-9e94-47b9-8d1e-4867950d210f
Category	Network activity
Type	ip-dst
Value	195.78.33.200
Tags	No tags

Attribute #15

UUID	5a0ac4d2-97a8-4b76-bf49-4e0d950d210f
Category	Network activity
Type	ip-dst
Value	50.116.54.16
Tags	No tags

Attribute #16

UUID	5a0ac4d2-1908-41f4-ae48-4aa8950d210f
Category	Network activity
Type	ip-dst
Value	212.83.166.45
Tags	No tags

Attribute #17

UUID	5a0ac4d2-2b14-4a7c-86d9-46cd950d210f
Category	Network activity
Type	ip-dst
Value	137.74.254.64
Tags	No tags

Attribute #18

UUID	5a0ac4d2-ae4c-4005-bd7b-4548950d210f
Category	Network activity
Type	ip-dst
Value	104.227.137.34
Tags	No tags

Attribute #19

UUID	5a0ac4d2-b178-4a7e-b14b-4a16950d210f
Category	Network activity
Type	ip-dst
Value	188.165.220.214
Tags	No tags

Attribute #20

UUID	5a0ac4d2-f5a0-4806-9b9f-4519950d210f
Category	Network activity
Type	ip-dst
Value	85.143.221.180
Tags	No tags

Attribute #21

UUID	5a0ac4d2-57c8-4d89-916f-486f950d210f
Category	Network activity
Type	ip-dst
Value	119.82.27.246
Tags	No tags

Attribute #22

UUID	5a0ac4d2-1a24-4ae0-a9fc-4823950d210f
Category	Network activity
Type	ip-dst
Value	194.88.246.7
Tags	No tags

Attribute #23

UUID	5a0ac4d2-8fb0-49d9-ae66-4eb7950d210f
Category	Network activity
Type	ip-dst
Value	206.214.220.79
Tags	No tags

Attribute #24

UUID	5a0ac4d2-debc-4839-80be-4b11950d210f
Category	Network activity
Type	ip-dst
Value	173.230.136.67
Tags	No tags

Attribute #25

UUID	5a0ac4d2-1068-4201-9cc0-4b86950d210f
Category	Network activity
Type	ip-dst
Value	173.224.218.25
Tags	No tags

Attribute #26

UUID	5a0ac521-3dfc-422a-b3fa-4d7c950d210f
Category	Persistence mechanism
Type	regkey
Value	%appdata%\roaming\microsoft\windows\start menu\programs\startup\[random].lnk
Tags	No tags

Attribute #27

UUID	5a0ac521-ca08-4726-bad0-4466950d210f
Category	Payload delivery
Type	filename
Value	%Appdata%\local\[random]\[random].exe

Tags	No tags

Attribute #28

UUID	5a0ac521-b370-4446-b84e-4bb2950d210f
Category	Persistence mechanism
Type	regkey
Value	%localappdata%\microsoft\windows
Tags	No tags

Attribute #29

UUID	5a0ac521-ab0c-4ac5-b31f-4cf5950d210f
Category	Payload delivery
Type	filename
Value	%WINDIR%\System32\netshedule.exe
Tags	No tags

Attribute #30

UUID	5a0ac577-0aec-403a-b697-4d69950d210f
Category	Payload delivery
Comment	Emotet downloader
Type	sha256
Value	4ce5366c7eef1fff1260d5d7a0aec72c1246621838bf8df07f4a6ab3e5369d96
Tags	No tags

Attribute #31

UUID	5a0ac577-90f4-482f-b813-4e55950d210f
Category	Payload delivery
Comment	Emotet malware
Type	sha256
Value	ffcb204da3ff72d268c8ac065c2e7cce5c65fafc2f549d92d0c280c6099bd440
Tags	No tags

Attribute #32

UUID	5a0ac577-9008-42f4-a39c-4dc9950d210f
Category	Payload delivery
Comment	Emotet malware
Type	sha256
Value	59639027a7fd487295bad10db896528ea223684e6595cae4ce9a0bec8d809087
Tags	No tags

Attribute #33

UUID	5a0ed8a4-6294-41ce-ae02-e7e802de0b81
Category	Payload delivery
Comment	Emotet malware - Xchecked via VT: 59639027a7fd487295bad10db896528ea223684e6595cae4ce9a0bec8d809087
Type	sha1
Value	9214359938285f26785f7eaf25a74dddea678065
Tags	No tags

Attribute #34

UUID	5a0ed8a4-8cbc-4980-a1c7-e7e802de0b81
Category	Payload delivery
Comment	Emotet malware - Xchecked via VT: 59639027a7fd487295bad10db896528ea223684e6595cae4ce9a0bec8d809087
Type	md5
Value	5aa9fa89cee3ffc4c3009e34db830de0
Tags	No tags

Attribute #35

UUID	5a0ed8a4-1f84-4696-a287-e7e802de0b81
Category	External analysis
Comment	Emotet malware - Xchecked via VT: 59639027a7fd487295bad10db896528ea223684e6595cae4ce9a0bec8d809087
Type	link
Value	https://www.virustotal.com/file/59639027a7fd487295bad10db896528ea223684e6595cae4ce9a0bec8d809087/analysis/1506215055/
Tags	No tags

Attribute #36

UUID	5a0ed8a4-1748-4308-a4e3-e7e802de0b81
Category	Payload delivery
Comment	Emotet malware - Xchecked via VT: ffcb204da3ff72d268c8ac065c2e7cce5c65fafc2f549d92d0c280c6099bd440
Type	sha1
Value	a33763608d07880c5ca31fd68e30355c04201c92
Tags	No tags

Attribute #37

UUID	5a0ed8a4-073c-4f4c-aea8-e7e802de0b81
Category	Payload delivery
Comment	Emotet malware - Xchecked via VT: ffcb204da3ff72d268c8ac065c2e7cce5c65fafc2f549d92d0c280c6099bd440
Type	md5
Value	03b933fb1b471d7710d82d8b3f6c62b1

Tags	No tags

Attribute #38

UUID	5a0ed8a4-a5ec-4828-9615-e7e802de0b81
Category	External analysis
Comment	Emotet malware - Xchecked via VT: ffcb204da3ff72d268c8ac065c2e7cce5c65fafc2f549d92d0c280c6099bd440
Type	link
Value	https://www.virustotal.com/file/ffcb204da3ff72d268c8ac065c2e7cce5c65fafc2f549d92d0c280c6099bd440/analysis/1510558151/
Tags	No tags

Attribute #39

UUID	5a0ed8a4-690c-47b9-8647-e7e802de0b81
Category	Payload delivery
Comment	Emotet downloader - Xchecked via VT: 4ce5366c7eef1fff1260d5d7a0aec72c1246621838bf8df07f4a6ab3e5369d96
Type	sha1
Value	82519982e32708e94c54ffce3c652714049a04f6
Tags	No tags

Attribute #40

UUID	5a0ed8a4-0868-42fa-ad0f-e7e802de0b81
Category	Payload delivery
Comment	Emotet downloader - Xchecked via VT: 4ce5366c7eef1fff1260d5d7a0aec72c1246621838bf8df07f4a6ab3e5369d96
Type	md5
Value	517d9598ac8aa0ef0cb7145ffd64805e
Tags	No tags

Attribute #41

UUID	5a0ed8a4-6c28-4f4a-8db3-e7e802de0b81
Category	External analysis
Comment	Emotet downloader - Xchecked via VT: 4ce5366c7eef1fff1260d5d7a0aec72c1246621838bf8df07f4a6ab3e5369d96
Type	link
Value	https://www.virustotal.com/file/4ce5366c7eef1fff1260d5d7a0aec72c1246621838bf8df07f4a6ab3e5369d96/analysis/1510180240/
Tags	No tags

Attribute #42

UUID	5a0ed8a4-fd94-4d5f-8e45-e7e802de0b81
Category	Payload delivery

Comment	Qakbot malware - Xchecked via VT: ca2d536b91b15e7fc44ec93bbed1f0f46ae65c723b8a4823253a2a91b8241f9a
Type	sha1
Value	74153fa3ca1a97b68fdd31fa02c3e16daa03ac59
Tags	No tags

Attribute #43

UUID	5a0ed8a4-1e1c-4eca-8532-e7e802de0b81
Category	Payload delivery
Comment	Qakbot malware - Xchecked via VT: ca2d536b91b15e7fc44ec93bbed1f0f46ae65c723b8a4823253a2a91b8241f9a
Type	md5
Value	54240940b30c9f21e006d87371f490e6
Tags	No tags

Attribute #44

UUID	5a0ed8a4-2ee8-44be-abd5-e7e802de0b81
Category	External analysis
Comment	Qakbot malware - Xchecked via VT: ca2d536b91b15e7fc44ec93bbed1f0f46ae65c723b8a4823253a2a91b8241f9a
Type	link
Value	https://www.virustotal.com/file/ca2d536b91b15e7fc44ec93bbed1f0f46ae65c723b8a4823253a2a91b8241f9a/analysis/1510257822/
Tags	No tags

Attribute #45

UUID	5a0ed8a4-4da0-47ea-9e6d-e7e802de0b81
Category	Payload delivery
Comment	Qakbot malware - Xchecked via VT: da00823090dae3dae452ddc8a4c2a3c087389b4aacf1f0c12d13c83c9fcaef9c
Type	sha1
Value	4c04c92cf88dc1a0cc4829229786ac50c1a51aa5
Tags	No tags

Attribute #46

UUID	5a0ed8a5-a0cc-446a-8c32-e7e802de0b81
Category	Payload delivery
Comment	Qakbot malware - Xchecked via VT: da00823090dae3dae452ddc8a4c2a3c087389b4aacf1f0c12d13c83c9fcaef9c
Type	md5
Value	692802635dbd973b7944ebc8dbc22e2a
Tags	No tags

Attribute #47

UUID	5a0ed8a5-2c5c-4318-9715-e7e802de0b81
Category	External analysis
Comment	Qakbot malware - Xchecked via VT: da00823090dae3dae452ddc8a4c2a3c087389b4aacf1f0c12d13c83c9fcaef9c
Type	link
Value	https://www.virustotal.com/file/da00823090dae3dae452ddc8a4c2a3c087389b4aacf1f0c12d13c83c9fcaef9c/analysis/1510111314/
Tags	No tags