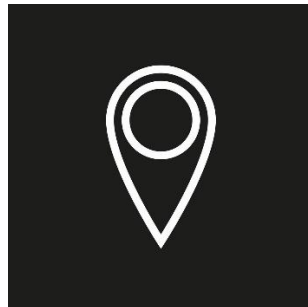




Wireshark Analysis

LAB ONE

Robert Christopherson | 9/18/2022 | Difficulty: Easy



Objective

A generated alert requires investigation to determine authenticity.

RT	1	2020-04-23...	119.31.234.40	80	10.0.0.167	51132	6	ET MALWARE Windows executable sent when remote host claims to send an image M3
----	---	---------------	---------------	----	------------	-------	---	--

Assess a pcap log and determine if this alert is a true positive or a false positive. This will require basic Wireshark capabilities.

Method

Basic enumeration.

- Used search query “kerberos.CNameString” to determine hostnames and show endpoints caught in this pcap capture.
- From this we can extract two machine IP addresses, hostnames, and current user.
 - 10.0.0.149 | DESKTOP-C10SKPY | alyssa.fitzgerald
 - 10.0.0.167 | DESKTOP-GRIONXA | elmer.obrien

Get Requests

- Wireshark search query: `http.request.method == GET && ip.addr == 10.0.0.149`
 - Device is running Windows 10 (Discovered from the User-Agent tag)
- Wireshark search query: `http.request.method == GET && ip.addr == 10.0.0.167`
 - Device is running Windows 10 (Discovered from the User-Agent tag)
 - Found a suspicious .ZIP file downloaded from 158.69.28.93
 - Ran the raw binary through VirusTotal.

http.request.uri contains .zip						
No.	Time	Source	Destination	Protocol	Length	Info
4817	116.799971	10.0.0.167	158.69.28.93	HTTP	532	GET /docs_q50/3183

Frame 4817: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface 0						
Ethernet II, Src: HewlettP_f5:37:e5 (ac:16:2d:f5:37:e5), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)						
Internet Protocol Version 4, Src: 10.0.0.167, Dst: 158.69.28.93						
Transmission Control Protocol, Src Port: 51114, Dst Port: 80, Seq: 1, Ack: 1, Len: 478						
Hypertext Transfer Protocol						
GET /docs_q50/318389448/Judgement_04222020_318389448.zip HTTP/1.1\r\nHost: play-astrite-q50vq...						

Result

- VirusTotal returned 23 hits indicating this .ZIP file is the QakBot Trojan (AKA: Qbot or Pinkslipbot).
- <https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/qakbot>
- With the confirmed positive result, appropriate steps can be taken to remove the malware and secure the systems affected.

23
/ 56

?

Community Score

23 security vendors and no sandboxes flagged this file as malicious

4e0e1d2b54ccdbb45aab9cc17cf6a3d756d1b411816dadbec88ff48c966e46fe
wiresharktest

93.53 KB
Size

2022-06-12 19:46:04 UTC
3 months ago

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis

ALYac	① VBS.Heur.Maltzur.1.38E625F8.Gen	Arcabit	① VBS.Heur.Maltzur.1.38E625F8.Gen
Avast	① VBS:Qakbot-D [Trj]	AVG	① VBS:Qakbot-D [Trj]
BitDefender	① VBS.Heur.Maltzur.1.38E625F8.Gen	Cynet	① Malicious (score: 99)
DrWeb	① Trojan.DownLoader33.37600	Emsisoft	① VBS.Heur.Maltzur.1.38E625F8.Gen (B)
eScan	① VBS.Heur.Maltzur.1.38E625F8.Gen	Fortinet	① VBS/Agent.TIV!tr.dldr
GData	① VBS.Heur.Maltzur.1.38E625F8.Gen	Ikarus	① Trojan-Downloader.VBS.Agent
Kaspersky	① HEUR:Worm.Script.Generic	Lionic	① Worm.Script.Generic.olc
MAX	① Malware (ai Score=81)	McAfee	① Artemis!32FCF9E1A298
McAfee-GW-Edition	① Artemis!32FCF9E1A298	Microsoft	① TrojanDownloader.VBS/Qakbot.AR!MTB
NANO-Antivirus	① Trojan.Script.ExpKit.fugogz	Sangfor Engine Zero	① Malware.Generic-VBS.Save.7eacba93
Trellix (FireEye)	① VBS.Heur.Maltzur.1.38E625F8.Gen	TrendMicro	① Trojan.VBS.QAKBOT.SM1
TrendMicro-HouseCall	① Trojan.VBS.QAKBOT.SM1	Acronis (Static ML)	✔ Undetected