KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | TA570 QBot Exploits Follina for Domain Compromise

Tracker ID: TN1108 **Date:** 09/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Background

A threat actor, possibly TA570, exploited the Follina vulnerability (CVE-2022-30190) to initiate a Qbot infection chain and obtain access to the systems. Qbot, also known as Qakbot or Pinksliplot, is a popular banking Trojan capable of several activities, including reconnaissance, lateral movement, data exfiltration, and delivery of additional payloads while acting as an initial access broker. Once the Qbot payload was run, the malware in an identified intrusion established C2 connectivity and performed discovery activity on the beachhead host. The threat actor moved laterally between numerous systems, set up remote management, and used Cobalt Strike to maintain network access.

The initial access in this attack was gained by a malicious Word document weaponized with Follina exploit code and supplied via a phishing email. When the Word document is executed, an HTML file containing a PowerShell payload is retrieved from a remote server. The payload is a base64-encoded code that downloads Qbot DLLs into the victim's Temp directory. Later, the Qbot DLL is executed via Regsvr32.exe and is injected into a trusted process (explorer.exe).

The injected process executes Windows commands such as whoami, net.exe, and nslookup to perform discovery operations and establish connections to Qbot C2 servers. To extract browser data, the threat actor also employed esentutl.exe, a Windows built-in program. As a technique of persistence, Qbot built a scheduled job that contained a PowerShell script that referenced a number of C2 IP addresses and was stored as base64-encoded blobs in keys with arbitrary names inside the HKCU registry hive. The threat actor then progressed to remote creation of Qbot DLL over SMB on other systems around the environment. To avoid detection, it added multiple directories to the Windows Defender exclusions list on each infected device, and the DLLs were then executed via remote services.

A Cobalt Strike server connection is established within the first hour of infection. The implanted Cobalt Strike process executed utilities such as nltest.exe and AdFind (explorer.exe). The injection method also enabled access to the LSASS system. The threat actors then installed NetSupport Manager, a remote management tool, and leveraged a Remote Desktop session to move laterally to the domain controller within 20 minutes of installation.

On the domain controller, Atera Remote Management, a popular program used by attackers to command victim PCs, was installed. The next day, the threat actors installed Network Scanner by SoftPerfect on a domain controller and performed a network port scan. Finally, the threat actors connected to one of the file-sharing servers using RDP to access confidential data. The breach lasted two days, and the attackers eventually expressed interest in accessing sensitive data kept on a file server before leaving the environment.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | TA570 QBot Exploits Follina for Domain Compromise

Tracker ID: TN1108 **Date:** 09/Nov/2022 **Category:** Vulnerability **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access , Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control

Detections

Utilize the below YARA rules to detect Follina infections in the network:

- Rule for process creation
- Domain Trust Discovery
- New Lolbin Process by Office Applications
- Sdiagnhost Calling Suspicious Child Process
- Registry Defender Exclusions
- Esentutl Steals Browser Information
- Network Reconnaissance Activity
- Atera Agent Installation
- FromBase64String Command Line
- Scheduled Task Executing Powershell Encoded Payload from Registry
- CobaltStrike Named Pipe
- SplashTop Network
- SplashTop Process

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link's target.
- Check the sender's identity. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- Continuously monitor for anomalous activities, including suspicious activity in the temp folder and the download or installation of unauthorized applications like Atera Remote Management and Network Scanner.
- Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | TA570 QBot Exploits Follina for Domain Compromise

Tracker ID: TN1108 **Date:** 09/Nov/2022 **Category:** Vulnerability **Industry:** All **Region**: All

References

- Follina Exploit Leads to Domain Compromise, The DFIR Report, 31st October 2022, External Link (thedfirreport.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | TA570 QBot Exploits Follina for Domain Compromise

Tracker ID: TN1108 **Date:** 09/Nov/2022 **Category:** Vulnerability **Industry:** All **Region:** All

*

URL	SHA256 Hash	SHA1 Hash	MD5	IP	IP	IP
www.stanzatextbooks[.]com	077ca8645a27c773d9c881aecf54bc409c2f8445ae8e3e90406434c09ace4bc2	3112a39aad950045d6422fb2abe98bed05931e6d	5abb2c12f066ce32a0e4866fb5bb347f	96[.]37[.]113[.]36:993	144[.]202[.]3[.]39:443	111[.]125[.]245[.]116:995
www.framemymirror[.]com	d20120cc046cef3c3f0292c6cbc406fcf2a714aa8e048c9188f1184e4bb16c93	03ef0e06d678a07f0413d95f0deb8968190e4f6b	e7015438268464cedad98b1544d643ad	93[.]48[.]80[.]198:995	67[.]209[.]195[.]198:443	39[.]49[.]96[.]122:995
www.coolwick[.]com	63315df7981130853d75dc753e5776bdf371811bcfce351557c1e45afdd1ebfb	dab316b8973ecc9a1893061b649443f5358b0e64	e7015438268464cedad98b1544d643ad	148[.]64[.]96[.]100:443	176[.]67[.]56[.]94:443	143[.]0[.]219[.]6:995
www.ajparts.co[.]uk				39[.]44[.]158[.]215:995	72[.]252[.]157[.]93:995	67[.]165[.]206[.]193:993
incredibletadoba[.]com				67[.]69[.]166[.]79:2222	90[.]120[.]65[.]153:2078	39[.]41[.]29[.]200:995
ibuonisani[.]it				45[.]63[.]1[.]12:443	72[.]252[.]157[.]93:990	191[.]112[.]25[.]187:443
gruposolel[.]com				31[.]48[.]174[.]63:2078	86[.]97[.]9[.]190:443	41[.]84[.]229[.]240:443
foxmotorent[.]com				196[.]203[.]37[.]215:80	37[.]34[.]253[.]233:443	80[.]11[.]74[.]81:2222
egofit.co[.]uk				144[.]202[.]3[.]39:995	23[.]111[.]114[.]52:65400	144[.]202[.]3[.]39:443
edifica[.]ro				1[.]161[.]101[.]20:443	190[.]123[.]44[.]126:443	217[.]164[.]121[.]161:1194
dwm-me[.]com				197[.]164[.]182[.]46:993	38[.]70[.]253[.]226:2222	89[.]86[.]33[.]217:443
cursosfnn[.]com				144[.]202[.]2[.]175:443	182[.]191[.]92[.]203:995	201[.]242[.]175[.]29:2222
cemavimx[.]com				5[.]203[.]199[.]157:995	37[.]186[.]54[.]254:995	31[.]35[.]28[.]29:443
atlasbar[.]net				217[.]165[.]79[.]88:443	140[.]82[.]63[.]183:443	124[.]109[.]35[.]32:995
				120[.]150[.]218[.]241:995	41[.]86[.]42[.]158:995	217[.]164[.]121[.]161:2222
				217[.]128[.]122[.]65:2222	89[.]101[.]97[.]139:443	39[.]44[.]213[.]68:995
				85[.]246[.]82[.]244:443	201[.]145[.]165[.]25:443	208[.]107[.]221[.]224:443
				94[.]71[.]169[.]212:995	173[.]21[.]10[.]71:2222	24[.]139[.]72[.]117:443
				177[.]205[.]155[.]85:443	82[.]41[.]63[.]217:443	47[.]157[.]227[.]70:443
				79[.]80[.]80[.]29:2222	73[.]151[.]236[.]31:443	175[.]145[.]235[.]37:443
				124[.]40[.]244[.]115:2222	149[.]28[.]238[.]199:443	63[.]143[.]92[.]99:995
				106[.]51[.]48[.]170:50001	83[.]110[.]218[.]147:993	149[.]28[.]238[.]199:995
				94[.]36[.]193[.]176:2222	86[.]195[.]158[.]178:2222	186[.]90[.]153[.]162:2222
				85[.]255[.]232[.]18:443	120[.]61[.]1[.]114:443	179[.]100[.]20[.]32:32101
				89[.]211[.]179[.]247:2222	140[.]82[.]49[.]12:443	190[.]252[.]242[.]69:443
				189[.]253[.]206[.]105:443	86[.]97[.]9[.]190:443	47[.]23[.]89[.]60:993
				69[.]14[.]172[.]24:443	92[.]132[.]172[.]197:2222	90[.]120[.]65[.]153:2078
				83[.]110[.]92[.]106:443	201[.]142[.]177[.]168:443	81[.]215[.]196[.]174:443
				72[.]252[.]157[.]93:995	82[.]152[.]39[.]39:443	70[.]46[.]220[.]114:443
				208[.]101[.]82[.]0:443	45[.]46[.]53[.]140:2222	76[.]25[.]142[.]196:443
				172[.]115[.]177[.]204:2222	71[.]24[.]118[.]253:443	41[.]38[.]167[.]179:995
				174[.]69[.]215[.]101:443	45[.]76[.]167[.]26:443	70[.]51[.]135[.]90:2222
				74[.]14[.]5[.]179:2222	144[.]202[.]2[.]175:995	67[.]209[.]195[.]198:443
				140[.]82[.]63[.]183:995	24[.]55[.]67[.]176:443	42[.]228[.]224[.]249:2222
				210[.]246[.]4[.]69:995	125[.]24[.]187[.]183:443	177[.]94[.]57[.]126:32101
				109[.]12[.]111[.]14:443	24[.]178[.]196[.]158:2222	104[.]34[.]212[.]7:32103
				148[.]0[.]56[.]63:443	187[.]207[.]131[.]50:61202	41[.]230[.]62[.]211:995
				121[.]7[.]223[.]45:2222	78[.]101[.]193[.]241:6883	177[.]209[.]202[.]242:2222
				47[.]156[.]131[.]10:443	202[.]134[.]152[.]2:2222	105[.]27[.]172[.]6:443
				40[.]134[.]246[.]185:995	103[.]246[.]242[.]202:443	46[.]107[.]48[.]202:443
				84[.]241[.]8[.]23:32103	39[.]52[.]41[.]80:995	86[.]98[.]149[.]168:2222
				75[.]99[.]168[.]194:443	187[.]251[.]132[.]144:22	173[.]174[.]216[.]62:443
				172[.]114[.]160[.]81:995	72[.]27[.]33[.]160:443	187[.]149[.]236[.]5:443
				75[.]99[.]168[.]194:61201	102[.]182[.]232[.]3:995	88[.]224[.]254[.]172:443
				108[.]60[.]213[.]141:443	176[.]67[.]56[.]94:443	45[.]76[.]167[.]26:995
				217[.]165[.]176[.]49:2222	201[.]172[.]23[.]68:2222	72[.]252[.]157[.]93:993
				177[.]156[.]191[.]231:443	37[.]34[.]253[.]233:443	197[.]89[.]8[.]51:443
				32[.]221[.]224[.]140:995	94[.]26[.]122[.]9:995	41[.]215[.]153[.]104:995
				76[.]70[.]9[.]169:2222	5[.]32[.]41[.]45:443	1[.]161[.]101[.]20:995
				179[.]158[.]105[.]44:443	91[.]177[.]173[.]10:995	117[.]248[.]109[.]38:21
				189[.]146[.]90[.]232:443	72[.]252[.]157[.]93:990	45[.]63[.]1[.]12:995

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia