Qbot Banking Trojan Still Up to Its Old Tricks

f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks

June 11, 2020

Attack Type:

Client-side Attacks

Attack Method:

Credential Theft

Attack Motive:

Cybercrime

Malware Type:

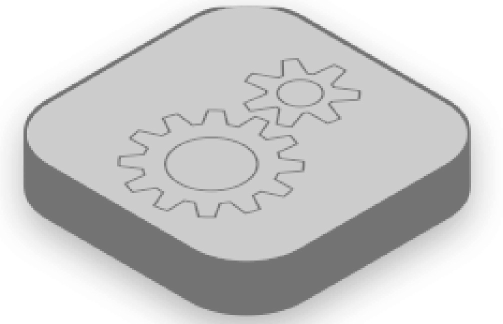
Trojan

Malware / Campaign Name:

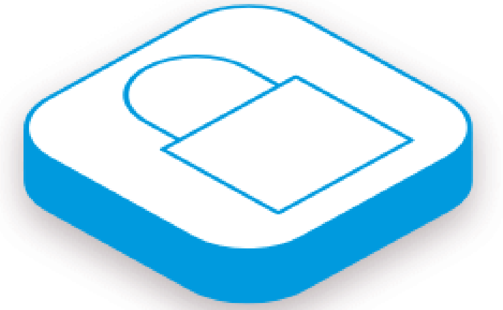
Qbot

App Tiers Affected:

Client

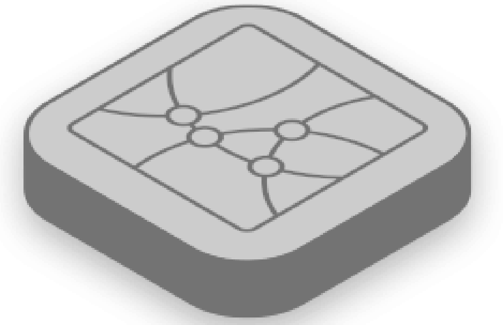


Services



Access

TLS



DNS

Network

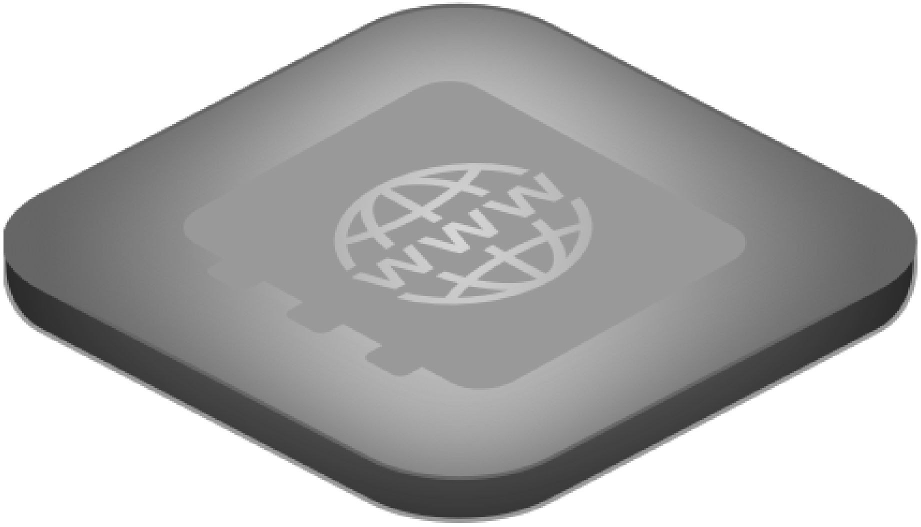
App Tiers Affected:

Client

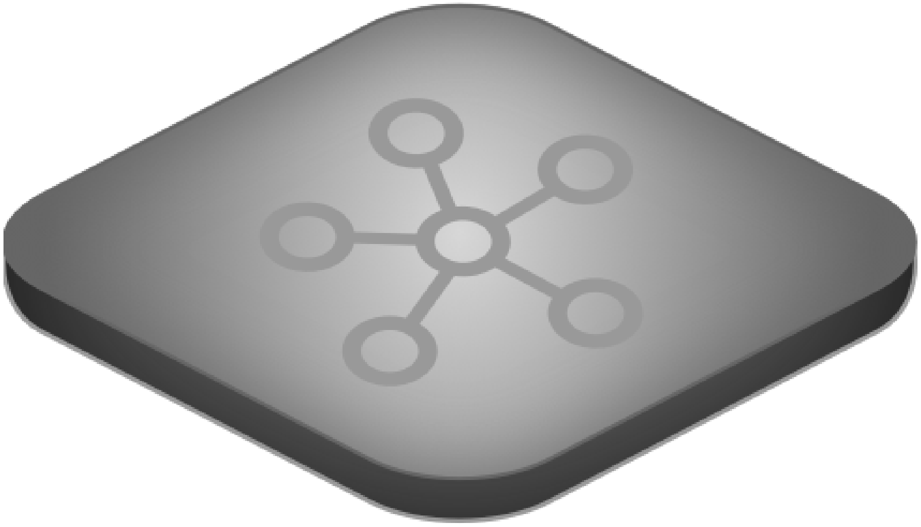
Services

Access

TLS



DNS



Network

There is no cease-fire in the continuing battle against malware. Qbot, a banking trojan malware active since 2008, is back in business with new functions and new stealth capabilities. In the past 12 years, this malware has gone by a handful of names, including Qakbot and Pinkslipbot.

Despite all the variations and evolutions, Qbot's main goal has remained the same: collect browsing activity and steal bank account credentials and other financial information. Attackers usually infect victims using phishing techniques to lure victims to websites that use exploits to inject Qbot via a dropper. It does this through a combination of techniques that subvert the victim's web sessions, including keylogging, credential theft, cookie exfiltration, and process hooking.

Previously, Qbot also used worm self-replication techniques to copy itself over shared drives and removable media. Qbot is still Windows-based, but this latest version adds both detection and research-evasion techniques. It has a new packing layer that scrambles and hides the code from scanners and signature-based tools. It also includes anti-virtual machine techniques, which helps it resist forensic examination. However, that didn't deter us analyzing its new capabilities and documenting the infection flow.

Qbot's Infection Process

Here's how the new Qbot infection typically occurs on a targeted computer:

1. Qbot is loaded into the running explorer.exe memory from an executable introduced via phishing, an exploit's dropper, or an open file share.
2. Qbot copies itself into the application folder's default location, as defined in the %APPDATA% registry key.
3. Qbot creates a copy of itself in the specific registry key **HKCU\Software\Microsoft\Windows\CurrentVersion\Run** to run when the system reboots.
4. Qbot drops a .dat file with a log of the system information and the botnet name.
5. Qbot executes its copy from the %APPDATA% folder and, to cover its tracks, replaces the originally infected file with a legitimate one.
6. Lastly, Qbot creates an instance of explorer.exe and injects itself into it. The attackers then use the always-running explorer.exe process to update Qbot from their external command-and-control server.

Qbot Web Banking Target List

Our latest analysis of several sample of the malware from this year showed that Qbot's focus is on banks in the United States. This appears to be a dedicated campaign with a browser hijack, or redirection, as the main attack method when the machine is infected. As Qbot watches a victim's web traffic, it looks for specific financial services from which to harvest credentials. We found specific strings within Qbot that targeted financial institutions, as shown in Table 1.

Target	Locale
https://*.jpmorgan.com/*logoff*	U.S.
https://*/cmserver/logout.cfm*	Any
https://express.53.com/express/logoff.action*	U.S.
https://businessaccess.citibank.citigroup.com/cbusol/quit.do*	U.S.
https://businessaccess.citibank.citigroup.com/cbusol/signOff.do*	U.S.
https://singlepoint.usbank.com/cs70_banking/logon/sbbExit/logout.do*	U.S.
https://*citizensbankmoneymanagergps.com/cb/servlet/cbonline/jsp/invalidate-session.jsp*	U.S.
https://www#.citizensbankmoneymanagergps.com/cb/servlet/cbonline/LogEZDExit*	U.S.
https://ktt.key.com/ktt/cmd/logoff*	U.S.
https://cashproonline.bankofamerica.com/cpwportal/terminateSession.jsp*	U.S.
https://top.capitalonebank.com/cashplus/security?*Logout*	U.S.
https://cbs.firstcitizensonline.com/cb/servlet/cbonline/invalidate-session.jsp*	U.S.
https://www.corporatebanking.firsttennessee.com/cb/servlet/cbonline/jsp/invalidate-session.jsp*	U.S.

https://otm.suntrust.com/stbcorp/logon/cpExit*	U.S.
https://ocm.suntrust.com/sunt/logon/sbbExit*	U.S.
https://e-access.compassbank.com/bbw/cmserver/logout.cfm*	U.S.
https://treasurydirect.soc.tdbank.com/bbw/cmserver/logout.cfm*	U.S.
https://wellsoffice.wellsfargo.com/ceoportal/framework/ceo_logout.jsp*	U.S.
https://*.ebanking-services.com/nubi/SignOut.aspx*	U.S.
https://*.ebanking-services.com/nubi/SignIn.aspx?timeout=y*	U.S.
https://business-eb.ibanking-services.com/K1/logout.jsp*	U.S.
https://business-eb.ibanking-services.com/K1/servlet/com.brokatfs.typhoon.htmlinf.servlet.CustLogoffServlet*	U.S.
https://tcfexpressbusiness.com/bbw/cmserver/logout.cfm*	U.S.
https://treas-mgt.frostbank.com/rdp/cgi-bin/logout*	U.S.
https://treas-mgt.frostbank.com/rdp/cgi-bin/welcome.cgi?loggedOff=True*	U.S.
https://businessonline.huntington.com/BOLHome/LogoutIntercept.aspx*	U.S.
https://businessonline.huntington.com/bolhome/BusinessOnlineAutoLogoff.aspx*	U.S.
https://webinfoplus.mandtbank.com/cashplus/security?requestID=Logout*	U.S.
https://businessonline.tdbank.com/CorporateBankingWeb/Core/SessionTimeout.aspx*	U.S.
https://businessonline.tdbank.com/CorporateBankingWeb/Core/Logout.aspx*	U.S.
https://www.scotiaconnect.scotiabank.com/scoui/pki/LogoutFromSCO.bns*	CA
https://www.firstmeritib.com/Logout.aspx*	U.S.
https://www.firstmeritib.com/cb/servlet/cbonline/jsp-ns/redirectFM.jsp?Page=Logoff*	U.S.
https://www.easterntreasuryconnect.com/bbw/cmserver/logout*	U.S.
https://*/wcmfd/wcmframework/TrapFunctionality?functionalityURL=/wcmfd/wcmframework/Signoff*	Any
https://*/wcmfd/wcmframework/Signoff*	Any
https://www.abnamro.nl/nl/logon/logoff.html*	Netherlands
https://*treasury.pncbank.com/TSCMCWeb/logoutMC.htm*	US
https://*/TMConnectWeb/cgi-bin/logoutconfirm.cgi*	Any
https://*/TMConnectWeb/cgi-bin/logout.cgi*	Any

https://*svbconnect.com/LogoutServlet/*	U.S.
https://*.web-cashplus.com/Cashplus/*Logout*	U.S.
https://*/cmserver/logout.cfm*	Any
https://weblink.websterbank.com/weblink/logout.asp*	U.S.
https://*/CLKCCM/*/exit.asp*	Any
https://*.secure.fundsxpress.com/piles/fxweb.pile/exit*	U.S.

Table 1. Financial institutions Qbot targets.

Regional Targeting by Qbot

Analysis of the latest Qbot campaign shows that it is mainly focused on the United States (see Figure 1), targeting approximately 36 U.S. financial institutions and two banks in Canada and the Netherlands; the rest of the list contains generic URL targets that might be added as a second stage in the fraud action.

Figure 1. Breakdown of Qbot redirection target list by country

Conclusion

Qbot has been around for a dozen years with pretty much the same functionality. The targets changed and features were added, but it’s still primarily about keylogging and, secondarily, about extracting a victim’s personal data. As Qbot waxes and wanes in popularity with attackers, it is hard to gauge its overall impact on a global scale. However, it is still a viable threat for defenders to be aware of.

Recommendations

- **Use updated antivirus software:** Antivirus software is still a powerful tool for detecting and stopping malware infections. Configure it to update its signatures without intervention and to alert you when it stops functioning.
- **Apply critical patches:** Apply critical patches for vulnerabilities with published, weaponized exploits for applications that touch the Internet, such as browsers and mail clients.
- **Inspect encrypted traffic:** Most malware and phishing sites are buried within encrypted SSL/TLS sessions, often using legitimate certificates. Decrypt, inspect, and sanitize this traffic.
- **Provide meaningful security awareness training:** Make it easy for users to report suspicious behavior. The F5 Labs 2018 Phishing and Fraud Report showed that training employees to recognize phishing attempts can reduce click-through rates on malicious emails, links, and attachments from 33% to 13%.

IOCs

⊕⊖

MD5

- 571cdef12082946e34b77bd50fcb0d38
- 06ec0af8411d864211baff8afb117f72
- 2d2fa093dd4fb26a8d14f1906552d238
- 842d7815923dffc1e1cf2ebbcd0fdf49
- 2e4c99684fc0046934b984268b16c25b

C2

hxxp://w1.plenimusic[.]com/fakes/