Menlo Labs Threat Bulletin

Bulletin: 2021-001

Date: 03/01/2021

Name: QBOT

Classification: Banking Trojan

Summary

In the last month, Menlo Labs has been tracking a malware campaign that is using services like Google Groups and Yahoo Mail to drop malicious ZIP files on to the endpoint. This campaign has been targeting customers in the Shipping, Financial and Defense verticals. This Malware is the QakBot/QBot Backdoor, which is known to steal user credentials.

Technical Details

Infection Vector

Web based Email and cloud services are the primary infection vector employed in this campaign. Since all of the sample hashes we discovered were hosted behind some form of authentication (Yahoo Mail / Google Groups), it was not possible to trace the kill chain for this attack. The ZIP files had social themes like Compensation Claim/Debt Details/Cancellation Notice etc.

Technical Analysis

Once the ZIP archive is downloaded onto the victim's endpoint:

- The ZIP file has a Macro laden Microsoft Excel file.
- Upon opening the Microsoft Excel file, the user is tricked into enabling the macro content.
- Upon running the Macro, an additional payload fetched and executed from a remote server.
- We found that this is usually a Malicious DLL payload that gets executed

IOCs:

Hashes (ZIP):

b46622ff5f5950a773d1f70d11bc66bbad4dc7554fc3c6dfeaca8a1d039e55ba

912bec8eeddad03136e702028e6bbe406991b9778aed530968d5bec203ecdf78

804532b0c42f7a67295d077f4c8c31748840be33e482681a0e0e1d48d6a4fe98

A074934d78c60bc6660dcf8822de857bda96d309e62173be6ccd4f17c47f8c8b

Hashes (DLL):

86a1bab21a568ec53689eaa30ca14ae5733251394c298b05d6ca8c07cf4d9a28

9bb3a1ea3332077e255a9da76a203336099964eac9e6423aa255dfcf1a8bfe2e

CNC Urls:

hxxp://bestivf.org/vttpaqt/416212.jpg

hxxp://biblicalisraeltours.com/ivqcapzu/987298.jpg

hxxp://cyberplanetghana.com/bxghdlyskp/987298.jpg

hxxp://dicomm-001-site35.ctempurl.com/pmslsda/44251820222106500000.dat

hxxp://dindorf.com.ar/ntpnttfypqs/44245986321643500000.dat

hxxp://gpccc.org/cjoxmc/416212.jpg

hxxp://gtrans.group/prduod/44252828044560200000.dat

hxxp://kevokloud.com/knrcqt/987298.jpg

hxxp://konyahaberler.xyz/hxjxxwav/44251820222106500000.dat

hxxp://loonytoys.com.ar/rqksqzjvcmv/416212.jpg

hxxp://miaovideo.com/wwdtfgdlijlr/44245692091203700000.dat

hxxp://nickdiehl.com/yzgglmktr/987298.jpg

hxxp://omnicomm.es/luuemiweb/416212.jpg

hxxp://outgrowmeinie.com/wcuiugnrebpk/44252828044560200000.dat

hxxp://oxcoz.com/nydprgwf/44252828044560200000.dat

hxxp://pandsquinny.com/nlbzyhfs/44251820222106500000.dat

hxxp://pricesrealized.fontainesauction.com/rqwapvpbj/987298.jpg

hxxp://rzminc.com/xklyulyijvn/44245763997106500000.dat

hxxp://sarayutseena-001-site1.gtempurl.com/kecljmkhyl/44252828044560200000.dat

hxxp://sharonbrockway.com/favohwn/44252828044560200000.dat

hxxp://slmtv.com/tfbgl/44251820222106500000.dat

hxxp://www.balkanstar.com/yzvegm/416212.jpg

hxxps://rzminc.com/xklyulyijvn/44245763997106500000.dat

MITRE ATT&CK Techniques:

command_and_control T1071

defense_evasion T1055

defense_evasion T1107

defense_evasion T1112

defense_evasion T1116

execution T1106

privilege_escalation T105

Conclusion:

Menlo Security's cloud security platform protects against this threat. Menlo labs proactively monitors threats and updates the platform accordingly with IOCs. IOCs in this campaign have been added to the product and are now categorized as malware. Customers are recommended to set their policy for threat categories, across isolated and application web requests, to block.

The Menlo cloud security platform has multiple content inspection engines that analyze and block such threats from reaching the endpoint.

Customers can choose to avail the below detection technologies to be integrated into the content inspection engine, providing defense in depth on a single platform.

- AV Engines
- Sandboxes

In addition to the above detection methodologies, the Menlo platform provides an additional layer of security against zero days and new malware campaigns by opening the document in safedocs and letting the customer download a safe version of the document.