Visa Security Alert

FEBRUARY 2017

FLOKIBOT MALWARE KIT TARGETS POS DEVICES IN LAC

Distribution: Issuers, Acquirers, Processors and Merchants

Summary: Multiple information security firms have reported on the emerging threat of a new malware variant identified as "Flokibot." Recently, two Flokibot campaigns compromised integrated point-of-sale (PoS) devices and other systems of multiple Brazilian merchants. Although we have no confirmation of other compromises, merchants in other countries—including Australia, Paraguay, Croatia, the Dominican Republic, Argentina, and the U.S.—were also reportedly targeted.

While Flokibot attacks have focused on the LAC region to date, this malware may represent a broader threat to the payments ecosystem. Visa is publishing this alert in order to provide clients and stakeholders with technical information, including background on the malware, indicators of compromise (IOC) and suggested mitigation activities to protect the payments ecosystem.

1. Recent Threat and Risk Description

Flokibot was first identified in the cybercrime underground in September 2016. The malware is comprised of source code from the ZeuS 2.0.8.9 Trojan, but incorporates a modified method for completing the malicious process injection (dropper). It does this in order to bypass anti-virus detection. In addition, Flokibot also employs a different network protocol than ZeuS that allows it to avoid detection by Deep Packet Inspection (DPI). The malware kit allows the Flokibot to feed configuration files in an encrypted state to its bots via Gate[.]php calls, as opposed to doing so in a separate payload (as in ZeuS). Similar to the ZeuS Trojan, the malware is designed to grab credit card data, and has recently targeted PoS devices in Brazil.

On 30 January 2017, it was reported that two Flokibot campaigns targeted 68 integrated PoS machines. One of the two campaigns specifically focused on Brazilian merchants, and reportedly compromised and exfiltrated card data. Once executed, Flokibot followed these steps to complete the infection and compromise:

- The initial infection vector is generally spearphishing attacks, in which victims are enticed to enable malicious macros in Microsoft Word documents sent as email attachments, or via exploit kits, such as RIG exploit kit.
- Once Flokibot is executed on the victim machine, it injects malicious code into "explorer.exe" – a Microsoft Windows file manager. If it is unable to inject in explorer.exe, it will then inject into "svchost.exe".
- The malware then performs two calls, the first to Sleep for 100 milliseconds, and the second passes control to another payload function.
- Flokibot has demonstrated the capability to use memory hooks to grab Track 2 data. It also incorporates a keylogging function.
- The language_id associated with recently reported victims was 1064 (Portuguese).

- In the two recent campaigns identified, other PoS malware, including DexterPOS, was also identified being deployed by the Flokibot operators on some of the compromised machines.
- Samples analyzed show Flokibot communicating with C2 infrastructure over an HTTPS connection.
    - The malware author advertises an "anti-deep packet inspection feature", similar to Zeus. However, security researchers decrypting the HTTPS found the malware currently sends back data to the infected machine (such as the computer name and the screen resolution) in clear text.
- Security researchers have identified support for command and control (C2) communication over the Tor network. Although samples analyzed did not reveal this functionality to be currently active, the malware checks for .onion based C2 URLs within the configuration file and would route the C2 traffic through a local Tor proxy (localhost:9050).

2. Best practices and mitigation measures

1. To identify Flokibot, scan networks for the following IOCs:

Indicator	Indicator Type
5028124ce748b23e709f1540a7c58310f8481e179aff7986d5cfd693c9af94da (SHA256)	Loader
08e132f3889ee73357b6bb38e752a749f40dd7e9fb168c6f66be3575dbbbc63d (SHA256)	File Hash
5028124ce748b23e709f1540a7c58310f8481e179aff7986d5cfd693c9af94da (SHA256)	File Hash
0aa1f07a2ebcdd42896d3d8fdb5e9a9fef0f4f894d2501b9cbbe4cbad673ec03 (SHA256)	File Hash
5e1967db286d886b87d1ec655559b9af694fc6e002fea3a6c7fd3c6b0b49ea6e (SHA256)	File Hash
d1d851326a00c1c14fc8ae77480a2150c398e4ef058c316ea32b191fd0e603c0 (SHA256)	File Hash
e0b599f73d0c46a5130396f81daf5ba9f31639589035b49686bf3ef5f164f009 (SHA256)	File Hash
e43ee2ab62f9dbeb6c3c43c91778308b450f5192c0abb0242bfddb8a65ab883a (SHA256)	File Hash
2b832ef36978f7852be42e6585e761c3e288cfbb53aef595c7289a3aef0d3c95 (SHA256)	File Hash
4bdd8bbdab3021d1d8cc23c388db83f1673bdab44288fccae932660eb11aec2a (SHA256)	File Hash
3c2c753dbb62920cc00e37a7cab64fe0e16952ff731d39db26573819eb715b67 (SHA256)	File Hash
7bd22e3147122eb4438f02356e8927f36866efa0cc07cc604f1bff03d76222a6 (SHA256)	File Hash
9d9c0ada6891309c2e43f6bad7ffe55c724bb79a0983ea6a51bc1d5dc7dccf83 (SHA256)	File Hash
e205a0f5688810599b1af8f65e8fd111e0e8fa2dc61fe979df76a0e4401c2784 (SHA256)	File Hash
ac5ae89af8d2ffdda465a4038f0f24fcbcb650140741c2b48adadc252a140e54 (SHA256)	File Hash
https[:]//193.201.225[.]30/sweetdream/gxve8xj4a7t8t8sug8s57.php	C2
https[:]//shhtunnel[.]at/class/gate.php	C2
https[:]//extensivee[.]bid/000L7bo11Nq36ou9cfjfb0rDZ17E7ULo_4agents/gate.php	C2
https[:]//5.154.190[.]248/gate.php	C2
https[:]//vtraffic[.]su/gate.php	C2
https[:]//springlovee[.]at/adm/config.bin	C2
https[:]//feed.networksupdates[.]com/feed/webfeed.xml	C2
https[:]//wowsupplier[.]ga/cpflkabwbebeu/gtlejbsbu.php	C2
https[:]//adultgirlmail[.]com/mail/gate.php	C2
https[:]//uspal[.]cf/3faf5c96-9c2b-11e6-95d4-00163c75bf83/gate.php	C2

2. More IOCs are also available here

3. Visa recommends the following best practices to reduce the risk of exposure:

a. Educate employees about avoiding phishing scams and safely opening emails with attachments.
b. Maintain a patch management program and update all software and hardware firmware to most current release, which limits the attack surface for zero-day vulnerabilities.
c. Turn on heuristics (behavioral analysis) on anti-malware to search for suspicious behavior.
d. Monitor for endpoints running TCP 9050 and monitor outbound network traffic communicating with known Tor exit node IP addresses.

e. Perform file integrity monitoring and alert on changes to explore.exe and svchost.exe processes on endpoints.
f. Monitor network traffic using a proxy.

4. Refer to the following resources for more information on security standards, PCI compliance requirements and best practices:
   a. PCI Data Security Standard Quick Reference Guide
   b. Refer to Visa's Card Acceptance Guidelines for Visa Merchants
   c. Additional information on PCI DSS can be found at www.pcissc.org.

Additional resources: Visa's What to Do If Compromised procedures

3. Sources

- https://www.arbornetworks.com/blog/asert/flokibot-invades-pos-trouble-brazil/
- https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/
- https://www.flashpoint-intel.com/flokibot-curious-case-brazilian-connector/
- http://blog.talosintelligence.com/2016/12/flokibot-collab.html
- https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/
- https://securityintelligence.com/news/floki-bot-funny-name-financial-nightmare/

For questions and additional information, please contact **paymentintelligence@visa.com**

To report a data breach, contact Visa Fraud Control:
- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Europe: Datacompromise@visa.com
- LAC: LACFraudInvestigations@visa.com
- U.S. and Canada: USFraudControl@visa.com