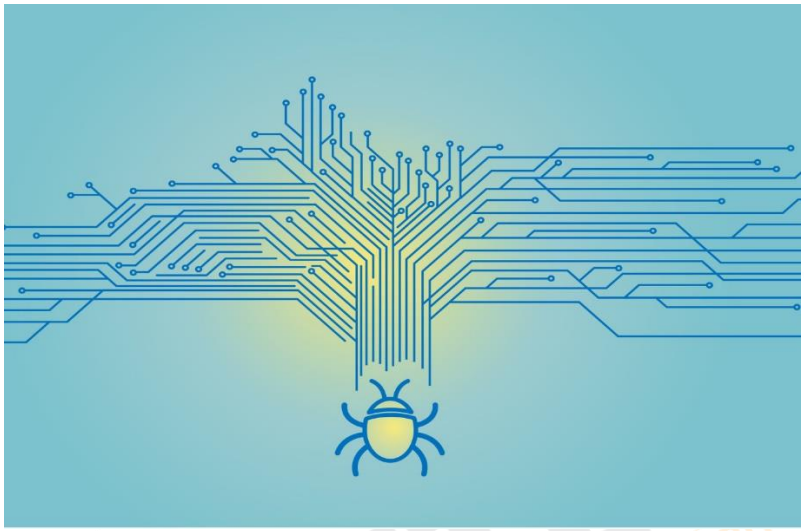
SEQURETEK

Bandook Malware

OVERVIEW



Thirteen years old malware Bandook variants once again targets multiple sectors. Dozens of digitally signed variants of this malware started to reappear in the threat landscape.

Its backdoor capability establishes contact with a remotely-controlled server to receive additional commands like capturing screenshots to carrying out various file-related operations.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
30th Nov 2020	v 1.0	Vidhi Patel	Cdr. Subhash Dutta

OVERVIEW

- Old malware **Bandook from 2007**, is once again **targeting multiple sectors** including government, financial, energy, food industry, healthcare, education, IT and legal institutions from Singapore, Cyprus, Chile, Italy, USA, Turkey, Switzerland, Indonesia and Germany.
- A campaign **Dark Caracal supported by Kazakh and Lebanese governments** is behind this new variants of malware.
- The malware establishes connection **with remotely-controlled server to receive additional commands** like capturing screenshots to carrying out various file-related operations.
- The malware has currently **three variants** are operated and sold by the operators.
  - A full-fledged version with 120 commands (not signed).
  - A full-fledged version (single sample) with 120 commands (signed).
  - A slimmed-down version with 11 commands (signed).
- Bandook is being sold to governments and threat actors worldwide, to facilitate offensive cyber operations.

TECHNICAL DETAILS

- Bandook infection process chain contains three phases. The process starts with a phishing Microsoft **word document with embedded code** delivered inside ZIP file format.
- Once opened, malicious **VBA macros are downloaded using the external template** via a URL shortening web service like TinyURL or Bitly.

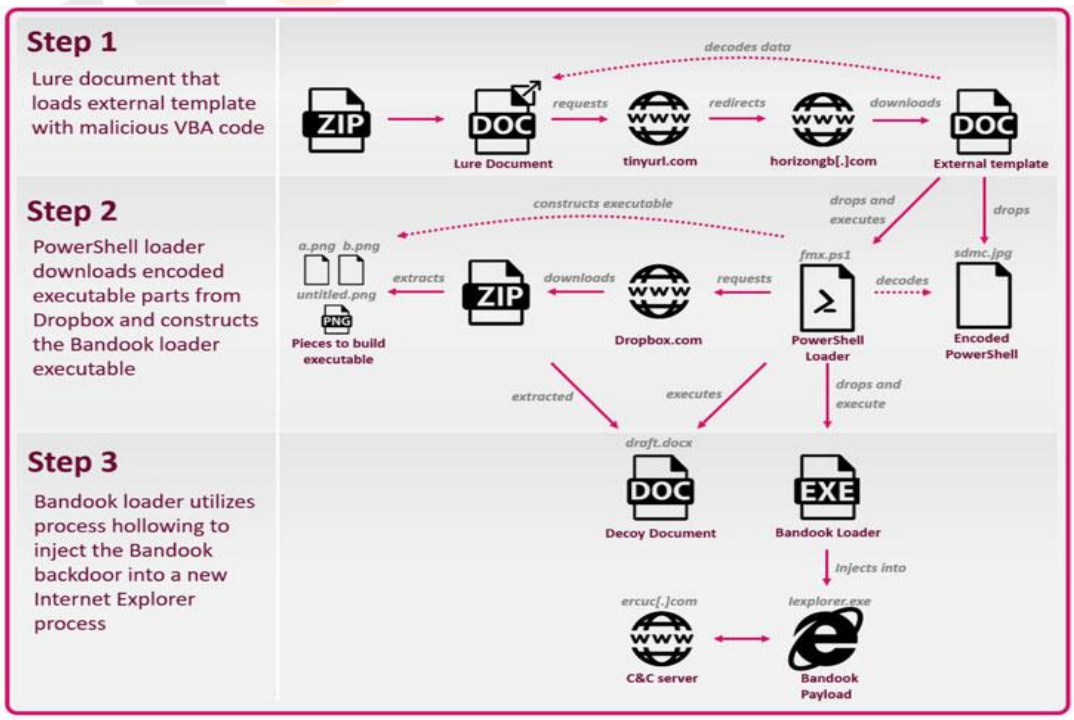


Figure 1: Bandook Infection Chain (source: Check Point)

- In second phase VBA macro **decrypts embedded code** in original document and drops the PowerShell loader script.
- This PowerShell script is used to download encoded executable parts from cloud storage services like Dropbox, Bitbucket or an S3 bucket in order to assemble the Bandook loader.
- In last phase, the loader written in Delphi uses the Process Hollowing technique to **create a new instance of an Internet Explorer process and injects a malicious Bandook payload** into it. The payload **contacts the C&C sever, sends basic information about the infected machine**, and waits for additional commands from the server.
- With new variants, operators have added layers of security, valid certificates, and other techniques to avoid detection.

INDICATORS OF COMPROMISE

DOMAINS

2ndprog[.]monster	htname[.]info	p2020[.]xyz	s3[.]megawoc[.]com
branchesv[.]com	idcmht[.]com	pronews[.]icu	styleco[.]me
d1[.]p2020[.]club	jtoolbox[.]org	raysdoor[.]com	tancredis[.]com
d2[.]p2020[.]club	mainsrv[.]top	s1[.]fikofiko[.]top	vdscloud[.]net
ec2[.]mbcde[.]net	mxtms[.]com	s1[.]megawoc[.]com	vsimperial[.]com
ercuc[.]com	nopejohn[.]com	s2[.]fikofiko[.]top	
ewsdocs[.]com	ntsclouds[.]com	s2[.]megawoc[.]com	
horizongb[.]com	olex[.]live	s3[.]fikofiko[.]top	

FILE HASHES (MD5)

045CE6679ED4086E2DED58470E24C15A	44584C8D010242FDDB44AFE5CE860872
0475771B8BC3EFC28B1834F3ADD608F3	4D7E67ED02713C789336F8804231B1CA
07111AFF7AFC052A81F267EA2E83DCEF	4D7E67ED02713C789336F8804231B1CA
07111AFF7AFC052A81F267EA2E83DCEF	4E9E12C98CFBC5F3AA3C1345BD063FA0
07776B2DD00BCD0BE1C7713C37D41120	53B7BDD75776F342BF5F5395D4C46520
17FE9611EA566887B3EF42284F96DE03	53B7BDD75776F342BF5F5395D4C46520
17FE9611EA566887B3EF42284F96DE03	54AD403349831B175A98A429F818F02A
1A3889DED73044F8BA0A00C2F089A3BD	54AD403349831B175A98A429F818F02A
27F8D8BBBEEDA5FC439EE18D9D4DA343	573C7DBF4D3AED421BFF58DF770610FE
28AD9ACE11919B57BF540E2B9DEBF8DD	5A3F7C46748791494E29383D1F58A908
3F310215A70D748F9335C767E61A2AB4	6EFFED1B1BB5E9ED6AAFACB075C1D4E2

70FF19341DEE7973EA6DD8E15C6BA86F	B9B8D6F46FF3A9058FFE4B304604B4E7
7C15EE5B9A12DACAACE8FB62271F12F1	BCA04D74261FEDFBD191FFD5E7CF6214
7EF261C151519E66EC369C63E4B1AED4	CFEA49C577EF865DE659D5B8025DB3F9
83311C960609418D5F0A5160324CEB1D	CFEA49C577EF865DE659D5B8025DB3F9
83311C960609418D5F0A5160324CEB1D	D1600F45005AA8B8FCBB446F34F7B9F5
96F09C5C56F59C733D1A9B01FEA0CFB4	D1600F45005AA8B8FCBB446F34F7B9F5
96F09C5C56F59C733D1A9B01FEA0CFB4	D22B31848B6F17EFC87D538DEDE2F2A7
9BCF889B14968C61DF95961A161719BA	D6E524514E0D112015C841B62377D648
9BCF889B14968C61DF95961A161719BA	EB402E8DD2CAE58476ACC8E697EE7171
A6501C62B3A6FFA8D028A88138FE509F	EB402E8DD2CAE58476ACC8E697EE7171
B5138C77983DBA10C4976C411161BBF9	F037F3961F7D9FE1EB7AFA889B556CB1
B5138C77983DBA10C4976C411161BBF9	

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- **Preventive Actions**
  - Block the IoCs in the corresponding security devices.
  - All these IoCs are combined in our Threat Intelligence Feed that is integrated with our SOC to provide proactive threat protection to our clients.
  - Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
  - Update your Operating system and software to latest version.
  - Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
  - Do not trust emails from untrusted source.
  - Do not open links and attachments from untrusted sources.
  - Back-up data, store it outside of network connection.
  - Use strong password and change it at regular interval. Use multi-factor authentication.
  - Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.

- Corrective Actions
  - If infected, disconnect the affected system from the Network.
  - Inform the Information Security Team.
  - Use antivirus or anti-malware software to clean the malware.