FastPOS Updates in Time for the Retail Sale Season

Appendix

TrendLabs Security Intelligence Blog

October 2016

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Related SHA1:

Detection	SHA1
TSPY_FASTPOS.A	8e7761e123026d9ce6a108e77dd677ee5d6245e4

Other Detections:

- TSPY64_FASTPOS.A
- TSPY_FASTPOS.SMA
- TSPY_FASTPOS.SMDRP

YARA Rule:

```
rule PoS_Malware_fastpos2 : FastPOS2
{
meta:
	author = "Trend Micro, Inc"
	date = "2016-09-21"
	description = "Used to detect newer FastPOS variants and their modules."
	sample_filetype = "exe"
strings:
	$pdb0 ="\\_hookLoader\\Release\\_hookLoader.pdb" nocase
	$pdb1 ="\\_hookKlg\\Release\\_hookKlg.pdb" nocase
	$pdb2 ="\\_hookKlg\\x64\\Release\\_hookKlg.pdb" nocase
	$pdb3 ="\\_hookProc\\Release\\_hookProc.pdb" nocase
	$pdb4 ="\\_hookProc\\x64\\Release\\_hookProc.pdb" nocase
	$pdb5 ="\\_hookRecvSrvc\\Release\\_hookRecvSrvc.pdb" nocase
	$exec_ref0 = "\\kl32.exe"
	$exec_ref1 = "\\servhelp.exe"
	$exec_ref2 = "\\kbd.exe"
	$exec_ref3 = "\\servproc.exe"
	$exec_ref4 = "\\service.exe"
	$exec_ref5= "\\proc64.exe"
	$exec_ref6 = "\\proc32.exe"
	$exec_ref7 = "//cdosys.php"
	$string0 = "DeleteService"
	$string1 = "CreateMailslotA"
	$string2 = "StartServiceCtrlDispatcherA"
	$string3 = "\\\\.\\mailslot\\trackslot"
	$string4 = "Can't install hook service"
	$string5 = " -r to remove hook." wide

condition:
	(any of ($pdb*)) and (3 of ($exec_ref*)) and (2 of ($string*))
}
```

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2016 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003