Alice: A Lightweight, Compact, No-Nonsense ATM Malware

Appendix

TrendLabs Security Intelligence Blog

December 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.

ATM Malware Family Characteristics

The following table summarizes the properties of various ATM malware families that we have encountered.

From 2007 To 2014

Family	**Skimer**	**Ploutus**	**Padpin**	**NeoPocket**
Discovery Year	2007	2013	2014	2014
“In-the-wild”	Yes	Yes	Yes	Yes
Country Affected	Russia, Ukraine, other EU countries	Mexico	Eastern Europe, South East Asia	Unknown
Manufacturer Targeted	Diebold	NCR	NCR	Diebold
Installation method on ATM	Unknown	CD-ROM	CD-ROM	Unknown
Family branches to multiple variants	Yes	Yes	No	No
Programming Language	Delphi	C# compiled into .NET	C# compiled into .NET	VB
Library used to access peripherals	DbdDevAPI.dll	ncr.aptra.axfs. activexfscontrols.dll	MSXFS.dll	Peripherals not accessed
Access control implemented	Yes	Yes	Yes	Yes
Dispenses cash	Yes	Yes	Yes	No
Steals information	Yes	No	No	Yes
User menu	Yes	Yes	Yes	No
User commands received via	PIN pad	Keyboard, PIN pad,SMS	PIN pad	Raw socket, files
Language Strings	Spanish	English, Spanish	English	Spanish
Encrypts stolen data	Yes	No	No	Yes
Time limited campaign	No	Needs activation every 24hrs	Operates only at certain times	Operates before May 21st, 2014
Persistent between reboots	Yes	Yes	Yes	Yes
Anti-Virus disabled	No	No	Yes (via other tool)	Yes
Disables ATM sensors	No	No	No	No

From 2015 To 2016

Family	Suceful	GreenDispenser	Ripper	Alice
Discovery Year	2015	2015	2016	2016
“In-the-wild”	No	Yes	Yes	Yes
Country Affected	N/A	Mexico	Thailand	Unknown
Manufacturer Targeted	Diebold, NCR (claimed)	Diebold/Nixdorf	Diebold/Nixdorf, NCR	Any
Installation method on ATM	N/A	Unknown	Unknown	USB or CD-ROM
Family branches to multiple variants	No	No	No	No
Programming Language	Borland C++	Visual C++	Visual C++	Undetermined
Library used to access peripherals	MSXFS.dll	MSXFS.dll	MSXFS.dll	MSXFS.dll
Access control implemented	No	Yes (two stage authentication)	Unconfirmed	Yes
Dispenses cash	No	Yes	Yes	Yes
Steals information	Yes	No	Unknown	No
User menu	Yes	Yes	Yes	Yes
User commands received via	Keyboard, Mouse	PIN pad	Keyboard, PIN pad, bank card (claimed)	Keyboard
Language Strings	Russian	English	English	English
Encrypts stolen data	No	No	No	No
Time limited campaign	No	Operates Jan 1st – Aug 31st 2015	No	No
Persistent between reboots	No	No	Yes	No
Anti-Virus disabled	No	No	No	No
Disables ATM sensors	Yes	No	No	No

Imported XFS Functions

Alice dynamically imports the following XFS API functions from the relevant DLLs:

Function Name	Description
WFSCleanUp	Disconnects an application from the XFS Manager

Function Name	Description
WFSOpen	Initiates a session between the application and the specified service
WFSGetInfo	Retrieves information from the specified service provider
WFSExecute	Sends a service-specific command to a service provider
WFSLock	Establishes exclusive control by call the application over the specified service
WFSRegister	Enables event monitoring for the specified service by the specified window
WFSFreeResult	Notifies the XFS Manager that a dynamically allocated memory buffer is to be freed
WFSUnlock	Releases a service that has been locked by a previous WFSLock function
WFSClose	Terminates a session between the application and the specified service
WFSStartUp	Establishes a connection between an application and the XFS Manager

Indicators of Compromise (IoCs)

The files used in this analysis have the following SHA256 hashes:

- B8063F1323A4AE8846163CC6E84A3B8A80463B25B9FF35D70A1C497509D48539
- 04F25013EB088D5E8A6E55BDB005C464123E6605897BD80AC245CE7CA12A7A70

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.

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