Dexter, Project Hook POS Malware Campaigns Persist

By Chris Brook

Published: 2014-03-06 · Archived: 2026-04-06 00:33:00 UTC

Research this week makes it's clear that many attackers are still using point of sale malware, namely Dexter and Project Hook, in active attacks.

While the Target data breach may be in the rear view mirror, research this week shows it's clear that many attackers are still using point of sale malware, namely Dexter and Project Hook, in active attacks.

Researchers at Arbor Networks' Security Engineering & Response Team (ASERT) looked at several such campaigns, exfiltrated data dumps and decoded them to analyze the scope of their compromises. The group also analyzed network activity triggered by Dexter malware samples.

According to Arbor's Threat Intelligence Brief 2014-3 released yesterday, researchers noticed a specific variation of Dexter, Dexter Revelation, exfiltrating stolen data, stored in fake .zip files and .txt files – via FTP credentials – from compromised terminals.

Revelation was one of three Dexter variants (along with Stardust and Millennium) that ASERT noticed in December but at that time it was unclear just how the infections were happening.

While researchers were under the assumption that Revelation was a fairly new brand of malware, new research has traced developmental versions of the malware back almost a year, early builds date back to April 2013.

It turns out the Revelation malware has several handy functions it uses including using a memory scraping procedure that "scours system memory looking for plaintext data that matches a credit or debit card format" and a keylogger function it uses to "capture keyboard activity and other system information." The fake .zip files store a four-byte XOR key that can actually be used to decode the file's contents.

The report suspects a threat actor going by either "Rome0" or "rome0" is directly involved with Dexter. Researchers say they've noticed actors going by both of the usernames demonstrating their familiarity with banking Trojans online and frequenting various carding forums.

ASERT posted a list of IP addresses and hostnames associated with Dexter's command and control activity in the report that it's hoping organizations review.

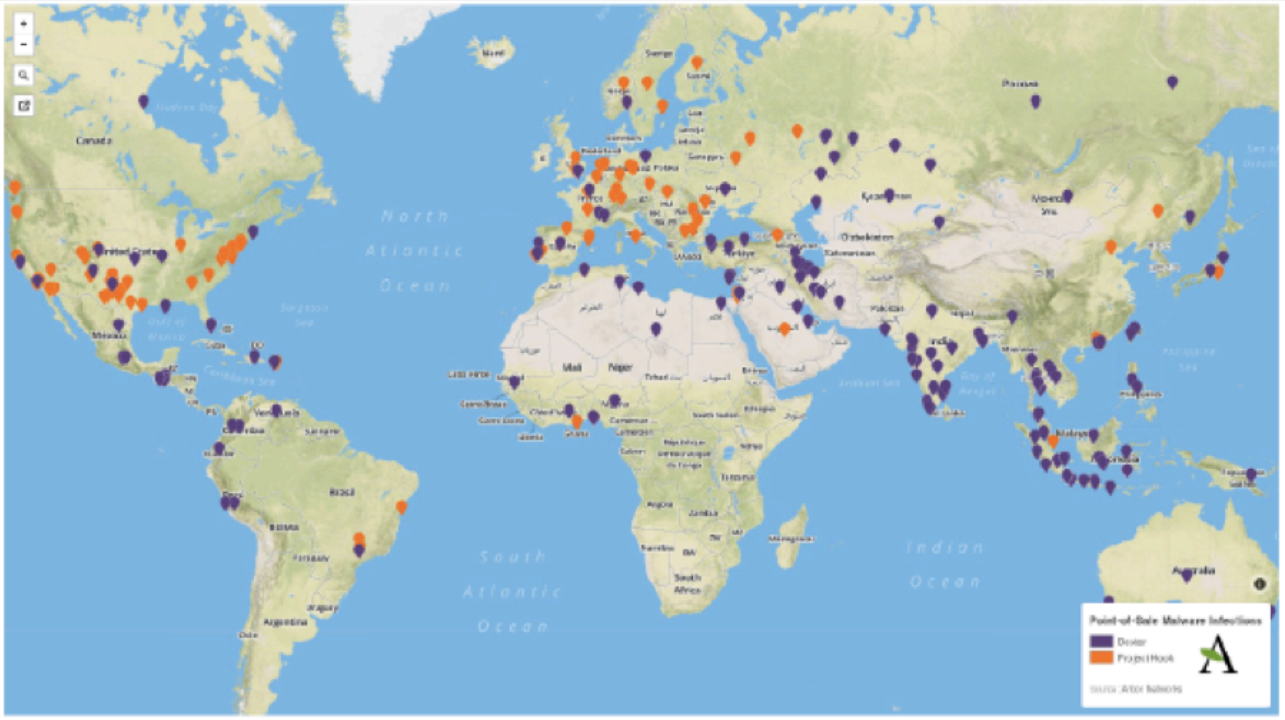
"Organizations are encouraged to check logs and other indicators of network activity associated with these IP addresses and/or hostnames to find systems compromised as part of a past or current attack campaign."

MD5	Port	Domain name	IP	Country	Timestamp
a0f799b2fbd6d485582aeeef2df513f7	80	hi.mybro.biz	141.105.67.87	RU	2013-11-01
347babe73944f5c99304344c4db2a53d	80	kongit.biz	198.50.197.47		2013-11-30
aab22d3b625ce47256fc47587e1a7cb6	80	**ursu.hol.es**	31.170.165.152	US	2014-02-07
77fb4eeec768f295493e7db71de09c07	80		**141.255.160.58 See NOTE 1**	CH	2014-01-28
140d24af0c2b3a18529df12dfbc5f6de	80		151.248.115.107	RU	2013-10-04
98faca3ad9d3cd668bb39e06d6e53707	80		**141.255.165.145**	CH	2014-01-27
fb9353ae0542439cd3dd1c260d215833	80	redirection67.net78.net	**31.170.162.103**	US	2014-01-21
caea1981c1cb071695f240a2270727ae	80	muia.ru	**176.9.207.177**	DE	2013-08-09

786659e3daf0ed2740b3b2cf2b568f3f	80	muia.ru	**176.9.207.177**	DE	2013-05-11
da98e6c0d497ba45aa6566d2eaabd2b5	80		**62.149.24.147**	UA	2014-02-05
a577b713802bb9e66ef61a5329d989b4	80	redirection67.net78.net	**31.170.162.103**	US	2014-01-22
7448bf7136c5e81305c1d1f668902807	80		**78.108.93.135**	RU	2014-02-09
c3a3d3cedfca895bbab07919b2aed7b5	80		62.76.44.111	RU	2013-07-23
5f5a388cf9e9682b2a527fe036b8dc1e	80	999andro.com	124.217.251.231	MY	2013-11-07
2afaa709ef5260184cbda8b521b076e1	80	hi.mybro.biz	**141.105.67.87**	RU	2013-11-01
94a13065468ddde1b3fea5112af8f1a4	80	hi.mybro.biz	**141.105.67.87**	RU	2013-11-02
d656494a72ce8a3fbc1d8b44f6695682	80		**141.255.160.58**	CH	2014-02-03
18af3ebfeed704edcf35f4a56723a85d	80		**89.45.14.69**	RO	2013-11-07
	21		**80.82.78.24** **See NOTE 2**	NL	
7b45730174853bf6dbe5ab197d80dc4a	80		**89.45.14.69**	RO	2014-01-10
	21		**80.82.78.24** **See NOTE 2**	NL	
1ec9f2118f2237a8d895dcb99012a47a	80	macar.na.tl	185.8.106.76	LT	2014-01-16
	21				
025f0ada53d517aa607ff3a248894329	21		**80.82.87.24**	NL	2013-12-21
	80		**89.45.14.69**	RO	
0d19afed3ad57de8caa8bf8802c45bf8	21		**80.82.87.24**	NL	2014-01-10
	80		**89.45.14.69**	RO	
60ac82aa228d6ba0d8d66bac70ad3c35	21		**80.82.87.24**	NL	2014-01-10
	80		**89.45.14.69**	RO	

The IP addresses listed in red indicate that the C&C servers associated with them were still active as of the report.

While Project Hook, another point-of-sale malware, is less active than Dexter, researchers are still encouraging organizations to remain vigilant especially after they found a special URL set up hosting back-end panels for Project Hook and another PoS malware: Alina, in January and early February.



Arbor's report came out the same day that Target announced it would finally overhaul its information security processes and that it's chief information officer, Beth Jacob, had resigned.

Target reports that it will fill the position with an external hire as well as assign a new role: chief compliance officer.

"Target will be conducting an external search for an interim CIO who can help guide Target through this transformation," Target's Chairman, President, and CEO Gregg Steinhafel said Wednesday.

The transformation Steinhafel is referring to is the stress the U.S. retailer has undoubtedly had to grapple with after suffering a massive breach in November. Attackers were able to set up a command and control server and lift more than 40 million credit and debit card records and 70 million other records of customer details from Target point of sale systems.

We may be three months removed from the Target fiasco but point-of-sale malware campaigns continue to permeate the headlines.

Texas-based Sally Beauty Supply, a chain with around 2,700 locations nationwide, confirmed yesterday that someone attempted to breach its system but would not confirm that customer data was at risk. According to Krebs on Security a batch of 282,000 stolen credit card numbers popped up on an underground market and three banks purchased their of their customers cards in hopes of finding the theft's origin. All of the banks then found that the cards they had gotten hold of had all been used at a Sally Beauty Supply store within 10 days before.

Source: https://threatpost.com/dexter-project-hook-pos-malware-campaigns-persist/104655/