

## GlitchPOS: New PoS malware for sale

By Paul Rascagneres

Published: 2019-03-13 · Archived: 2026-04-05 13:08:57 UTC



Wednesday, March 13, 2019 10:52

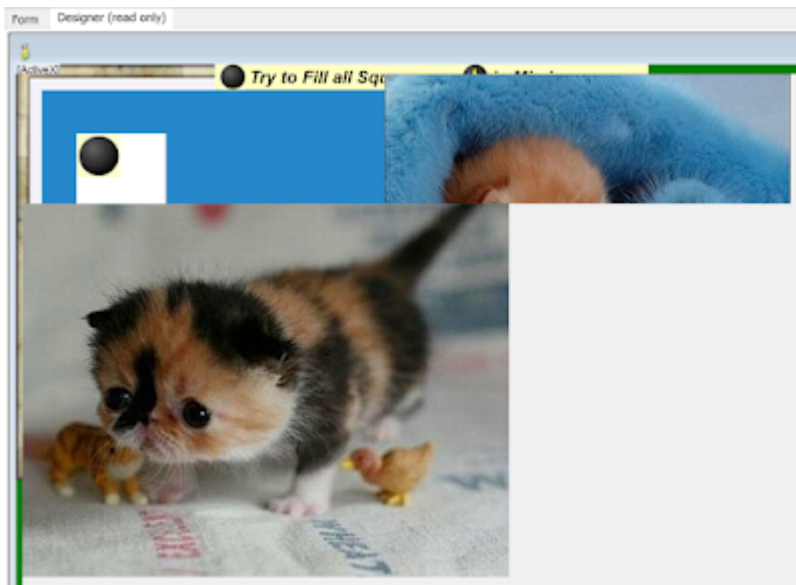
[Warren Mercer](#) and [Paul Rascagneres](#) authored this post with contributions from Ben Baker.

The actor behind this malware created a video, which we embedded below, showing how easy it is to use it. This is a case where the average user could purchase all the tools necessary to set up their own credit card-skimming botnet.

### GlitchPOS

#### Packer overview

**A packer developed in VisualBasic protects this malware. It's, on the surface, a fake game. The user interface of the main form (which is not displayed at the execution) contains various pictures of cats:**



The purpose of the packer is to decode a library that's the real payload encoded with the UPX packer. Once decoded, we gain access to GlitchPOS, a memory grabber developed in VisualBasic.

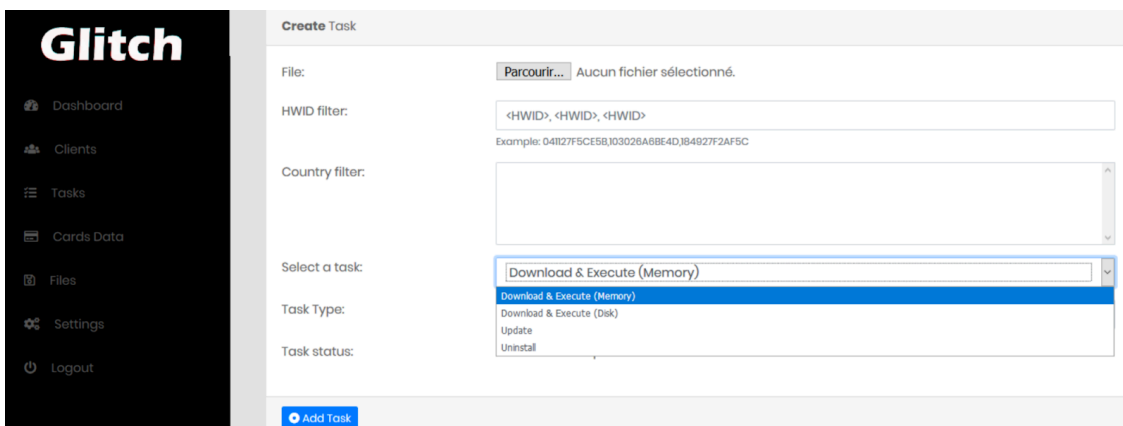
### Payload analysis

**The payload is small and contains only a few functions. It can connect to a command and control (C2) server to:**

- Register the infected systems
- Receive tasks (command execution in memory or on disk)
- Exfiltrate credit card numbers from the memory of the infected system
- Update the exclusion list of scanned processes
- Update the "encryption" key
- Update the User Agent
- Clean itself

### Tasks mechanism

**The malware receives tasks from the C2 server. Here is the task pane:**





## Credit card grabber

The main purpose of this malware is to steal credit card numbers (Track1 and Track2) from the memory of the infected system. GlitchPOS uses a regular expression to perform this task:

```
loc_4034F4: If arg_10 Then
loc_403502: var_90.Pattern = ";\d{13,19}=\d{7}\w*\"
loc_403509: Else
loc_40351B: var_90.Pattern = CVar("(" & Chr(37) & "B)\d{0,19}^\[w\s\/]{2,26}^\d{7}\w*\" & ";\d{13,19}=\d{7}\w*\"")
loc_403522: End If
loc_40352D: var_90.IgnoreCase = True
loc_40353A: var_90.Global = True
loc_403563: For Each var_94 In var_90.Execute
loc_403574: var_9C = CStr(var_94.Value)
loc_40357F: Next
```

- (%B)\d{0,19}^\[w\s\/]{2,26}^\d{7}\w\*\"?

The purpose of this regular expression is to detect Track 1 format B

Here is an example of Track 1:

Cardholder : M. TALOS

Card number\*: 1234 5678 9012 3445

Expiration: 01/99

%B1234567890123445^TALOS/M.

- ;\d{13,19}=\d{7}\w\*\"?

The purpose of this regular expression is to detect Track 2

Here is an example of Track 2 based on the previous example:

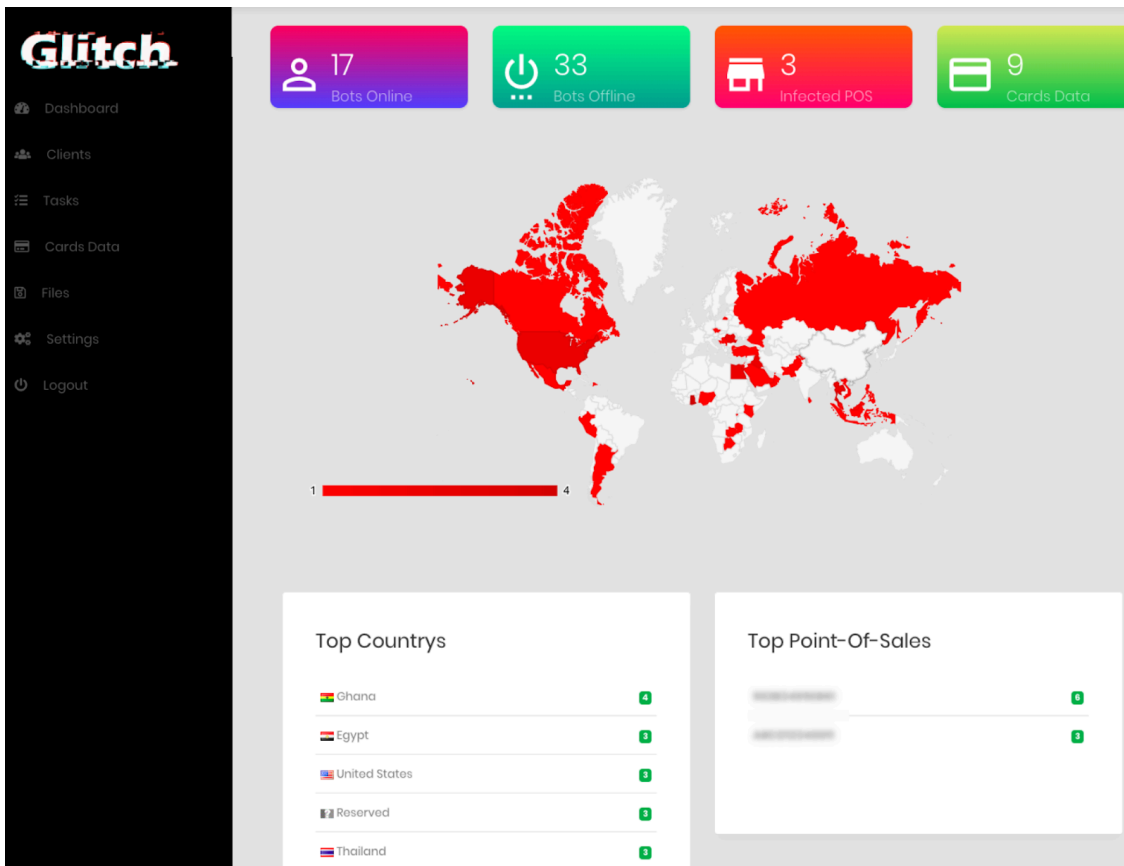
;1234567890123445=99011200XXXX00000000?\*

If a match is identified in memory, the result is sent to the C2 server. The malware maintains an exclusion list provided by the server. Here is the default list: chrome, firefox, iexplore, svchost, smss, csrss, wininit, steam, devenv, thunderbird, skype, pidgin, services, dwn, dllhost, jusched, jucheck, lsass, winlogon, alg, wscntfy, taskmgr, taskhost, spoolsv, qml, akw.

## Panel

Here are some additional screenshots of the GlitchPOS panel. These screenshots were provided by the seller to promote the malware.

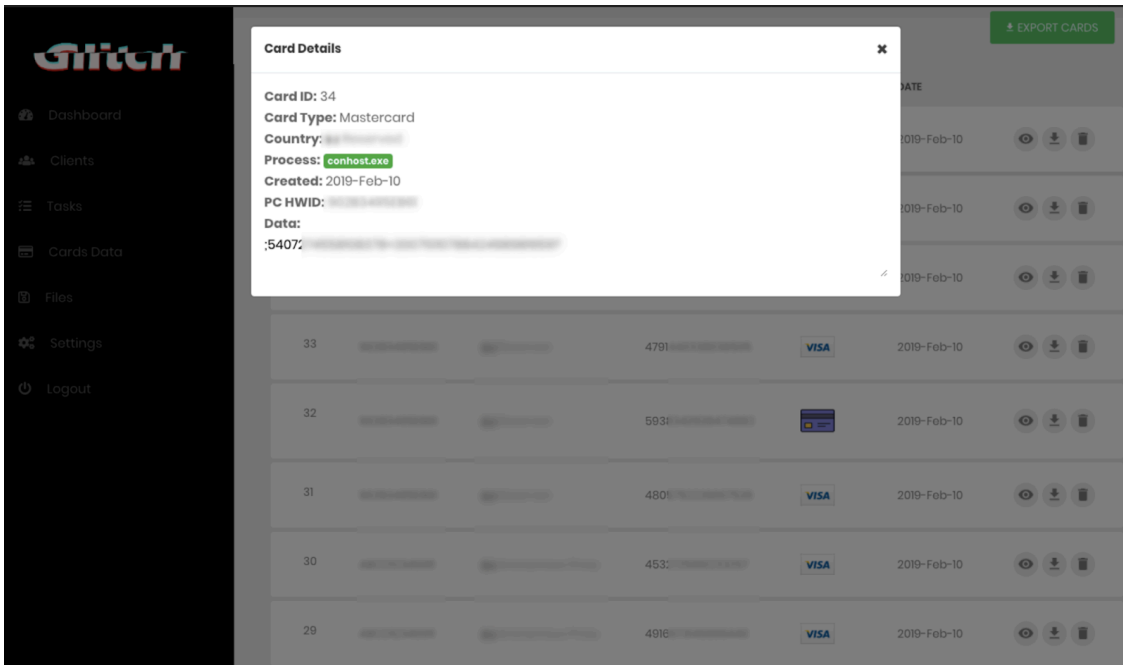
The "Dashboard:"



The "Clients" list:

HWID	IP	Country	PC-NAME	Cards	Status
9203449980	95.226.73.62	[Redacted]	95.226.73.62-PC	0	Offline
4822234609	5.82.99.95	[Redacted]	5.82.99.95-PC	3	Offline
5498233390	193.50.95.41	Czech Republic	JOHN-PC	0	Offline
5993294828	104.42.127.205	Thailand	DESKTOP-Q7RTRPG	0	Offline
7842442392	193.108.92.93	Malaysia	QX-PC	0	Online
9272246246	40.252.22.76	Kenya	HQICTDWK02379	0	Offline
3248274829	40.252.16.97	Ghana	DESKTOP-1PLEKSO	0	Offline
9291827434	194.227.146.223	Egypt	MAGIC-PC	0	Online
9822787870	24.68.274.0	Canada	TENEISHA-PC	0	Online

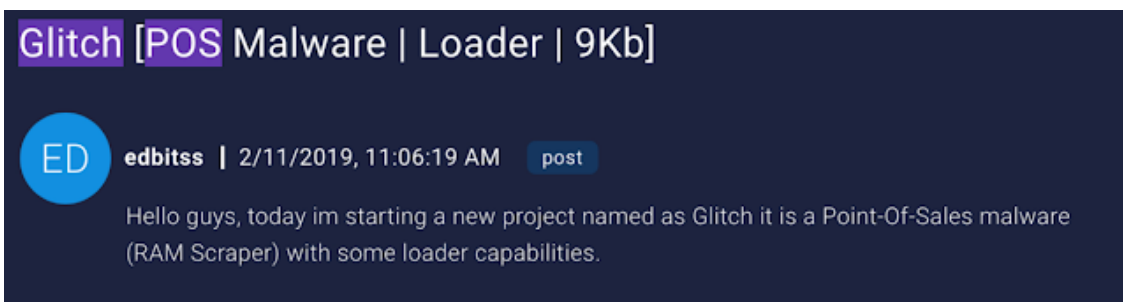
The "Cards Date:"



## Linked with DiamondFox L!NK botnet

**Author: Edbitts**

**The first mention of GlitchPOS was on Feb. 2, 2019 on a malware forum:**



Edbitts is allegedly the developer of the DiamondFox L!NK botnet in 2015/2016 and 2017 as explained in a report by [CheckPoint](#).

The screenshot shows a forum profile for a user named 'edbitss'. The profile includes a header with the username, role 'Lurker', and UID '1930893'. Below this is a profile picture of an eye in a triangle and a yellow 'MEMBER' badge. A status bar indicates the user is 'OFFLINE'. The 'Statistics' section shows 0 posts, 0 threads, 0 leecher value (Neutral), 0 likes, 0 reputation, and a low warning level. The 'Information' section lists the user's join date as 08-01-18 and last visit as Jan 16 2018 05:55 PM. The 'Signature' section features a 'DiamondFox' logo on a dark blue background.

The screenshot shows a forum post by 'edbitss', titled 'Vendor Of DiamondFox'. The post begins with 'Hello guys, im really happy to start a sales thread of the new DiamondFox version:'. The post is divided into sections: 'Panel:', 'Builder:', 'Loader:', and 'Plugins:'. The 'Loader:' section lists several features such as 'Core totally recoded', 'Stability Improved', and 'Full windows compatibility (x86 and x64 from XP to Windows 10)'. The 'Plugins:' section lists various tools like 'Browsers Password Stealer', 'FTP Stealer', and 'DDoS (UDP, Layer7 [3 Methods], HTTP)'. The post ends with 'Post: #1'.

The developer created this video to promote GlitchPOS, as well. In this video, you can see the author set up the malware and capture the data from a swiped card. We apologize for the quality, shakiness, music, and generally anything else with this video, again, it's not ours.

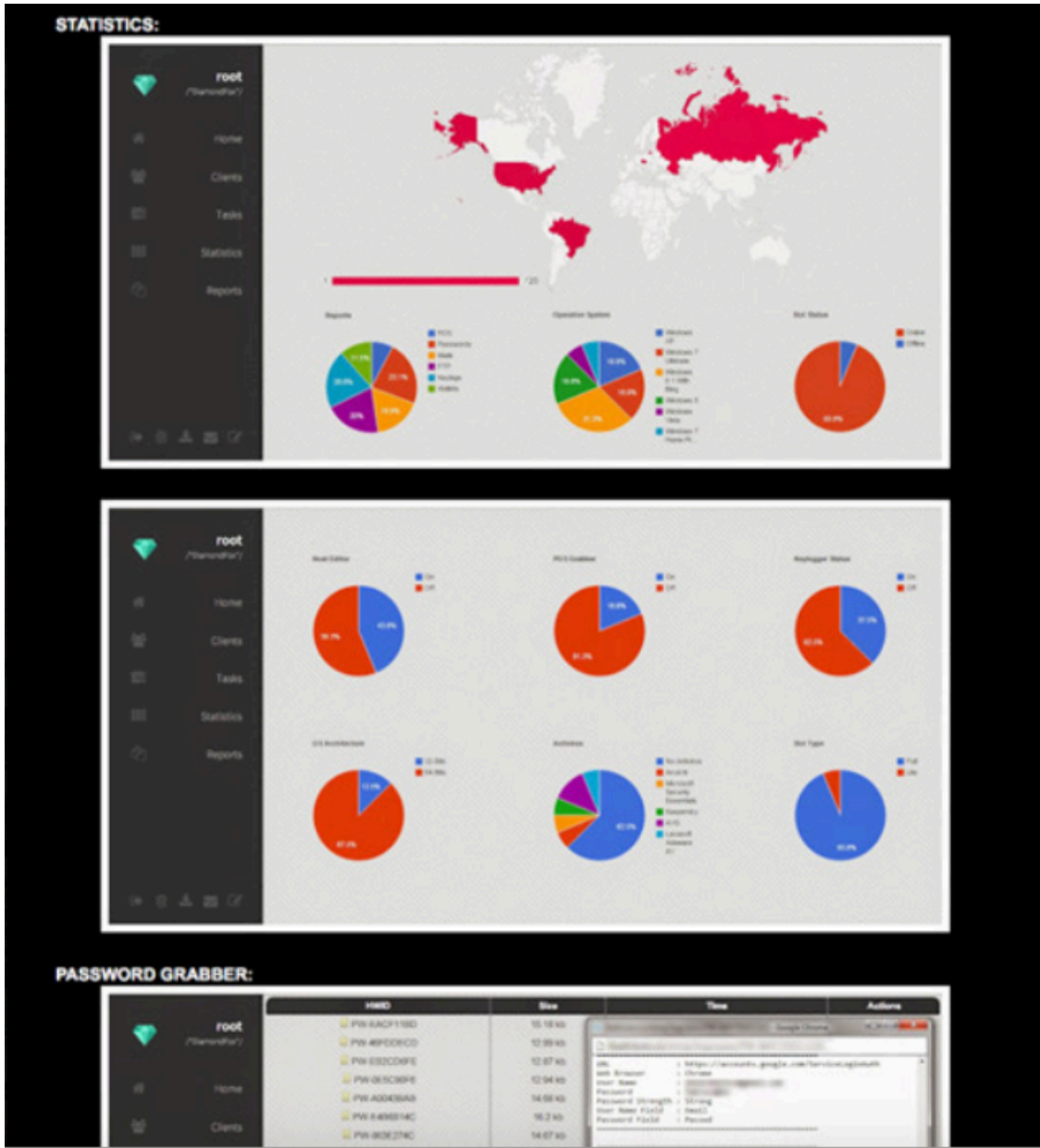
The built malware is sold for \$250, the builder \$600 and finally, the gate address change is charged at \$80.

## Panel similarities

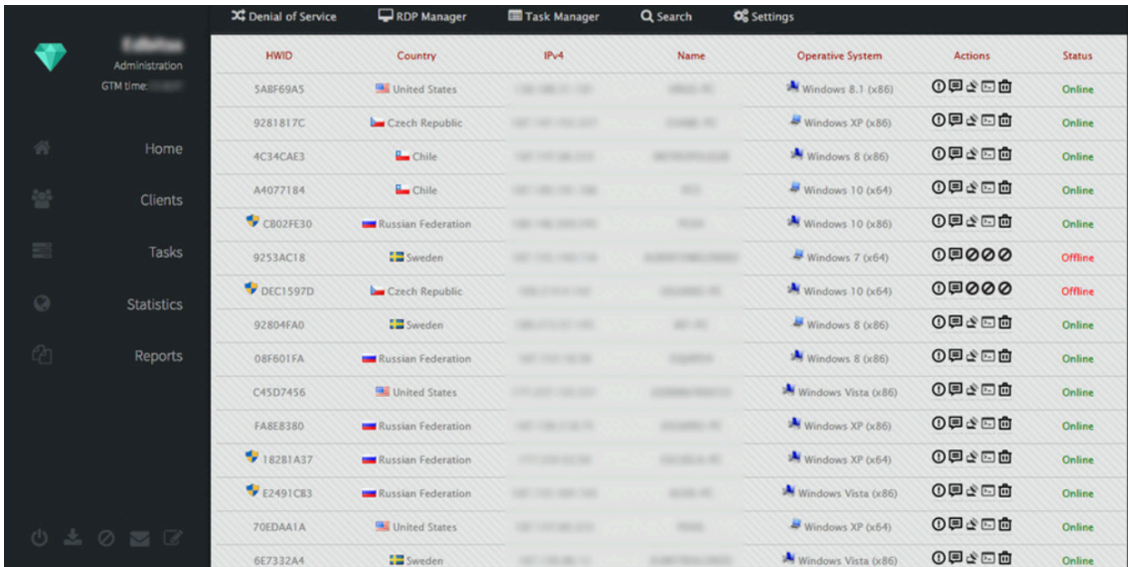
In addition to the malware language (VisualBasic), we identified similarities between the

**DiamondFox panel and the GlitchPOS panel. In this section, the DiamondPOS screenshots come from the CheckPoint report mentioned previously.**

Both dashboards' world map are similar (image, code and color):



The author used the same terminology such as "Clients" or "Tasks" on the left menu:



HWID	Country	IP-v4	Name	Operative System	Actions	Status
5ABF69A5	United States	192.168.1.101	192.168.1.101	Windows 8.1 (x86)	🔍 🗑️ 🔄 📄	Online
9281817C	Czech Republic	192.168.1.102	192.168.1.102	Windows XP (x86)	🔍 🗑️ 🔄 📄	Online
4C34CAE3	Chile	192.168.1.103	192.168.1.103	Windows 8 (x86)	🔍 🗑️ 🔄 📄	Online
A4077184	Chile	192.168.1.104	192.168.1.104	Windows 10 (x64)	🔍 🗑️ 🔄 📄	Online
CB02FE30	Russian Federation	192.168.1.105	192.168.1.105	Windows 10 (x86)	🔍 🗑️ 🔄 📄	Online
9253AC18	Sweden	192.168.1.106	192.168.1.106	Windows 7 (x64)	🔍 🗑️ 🔄 📄	Offline
DEC1597D	Czech Republic	192.168.1.107	192.168.1.107	Windows 10 (x64)	🔍 🗑️ 🔄 📄	Offline
92804FA0	Sweden	192.168.1.108	192.168.1.108	Windows 8 (x86)	🔍 🗑️ 🔄 📄	Online
08F601FA	Russian Federation	192.168.1.109	192.168.1.109	Windows 8 (x86)	🔍 🗑️ 🔄 📄	Online
C45D7456	United States	192.168.1.110	192.168.1.110	Windows Vista (x86)	🔍 🗑️ 🔄 📄	Online
FA8E8380	Russian Federation	192.168.1.111	192.168.1.111	Windows XP (x86)	🔍 🗑️ 🔄 📄	Online
182B1A37	Russian Federation	192.168.1.112	192.168.1.112	Windows XP (x64)	🔍 🗑️ 🔄 📄	Online
E2491C83	Russian Federation	192.168.1.113	192.168.1.113	Windows Vista (x86)	🔍 🗑️ 🔄 📄	Online
70EDA41A	United States	192.168.1.114	192.168.1.114	Windows XP (x64)	🔍 🗑️ 🔄 📄	Online
6E7332A4	Sweden	192.168.1.115	192.168.1.115	Windows Vista (x86)	🔍 🗑️ 🔄 📄	Online

The icons are the same too in both panels, as well as the infected machine list (starting with the HWID). The PHP file naming convention is similar to DiamondFox, too.

The author clearly reused code from DiamondFox panel on the GlitchPOS panel.

### Comparison of GlitchPOS and the DiamondFox POS module

**In 2017, the DiamondFox malware included a POS plugin. We decided to check if this module was the same as GlitchPOS, but it is not. For DiamondFox, the author decided to use the leaked code of BlackPOS to build the credit card grabber. On GlitchPOS, the author developed its own code to perform this task and did not use the previously leaked code.**

### Bad guys are everywhere

**It's interesting to see that someone else attempted to push the same malware 25 days after edbitss on an alternative forum:**

GLITCH | POS MALWARE | LOADER | 9kb

02-27-2019, 03:44 AM

GLITCH POINT OF SALE MALWARE

Hello friends

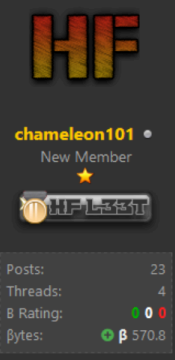
I bring to your attention "GLITCH" a professional pos malware.

**FEATURES:**

- File size: 9kb (10kb with configurations).
- Grab Track1 and Track2 Data.
- No dependencies.
- Persistence ( persists in pos terminal for a long time)
- File tested from XP to W10 (x86 and x64).
- Communication between loader and panel are encrypted.
- Configurations encrypted and mixed inside the loader.
- Fully compatibility with crypters.
- Non common way to get commands from the panel (bypass AVs).
- File melted after execution.
- Loader detects human activity to execute the payload (avoid analysis).

Panel:

Dashboard:

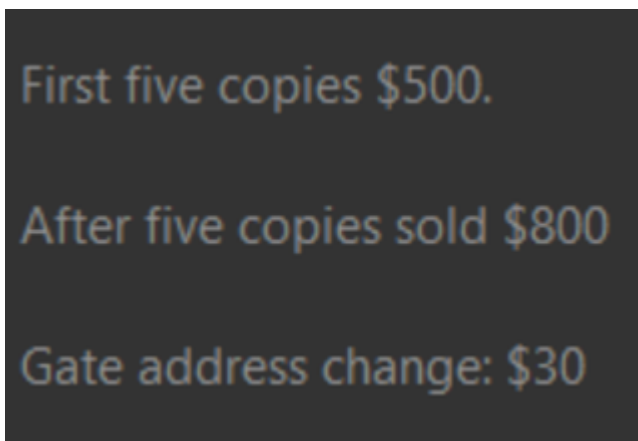


**HF**

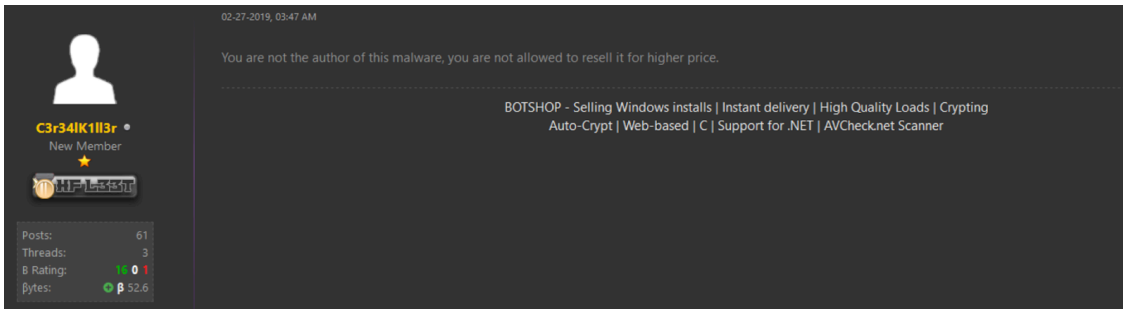
**chameleon101**  
New Member

Posts: 23  
Threads: 4  
B Rating: 0 0  
Bytes: 570.8

This attacker even tried to cash in by increasing some prices.



Some members even attempted to call out the unscrupulous behaviour:

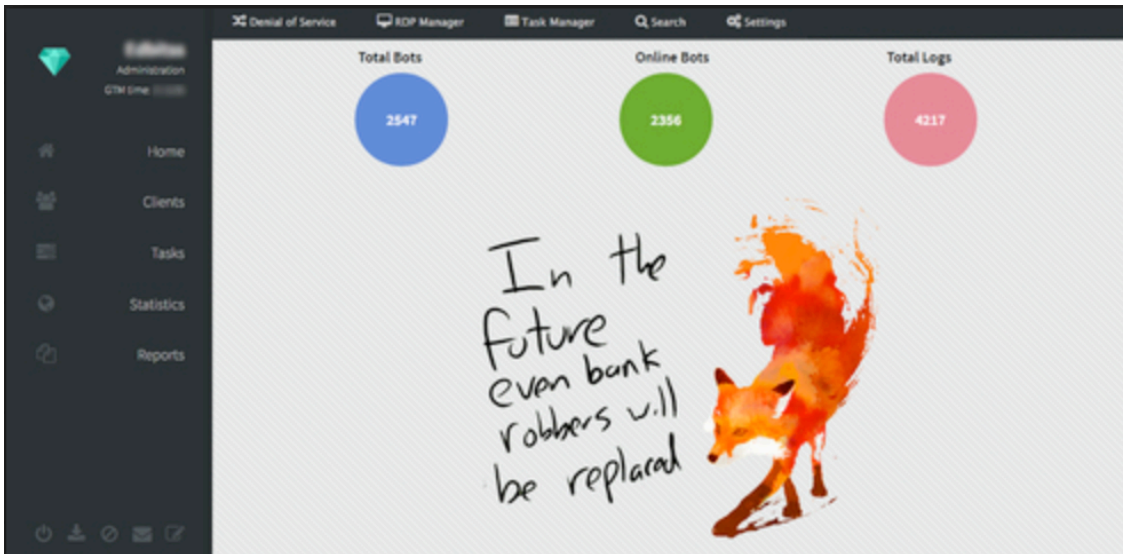


With the different information we have, we think that Chameleon101 has taken the previous malware created by Edbitts to sell it on an alternative forum and with a higher price.



## Conclusion

**This investigation shows us that POS malware is still attractive and some people are still working on the development of this family of malware. We can see that edbitss developed malware years even after being publicly mentioned by cybersecurity companies. He left DiamondFox to switch on a new project targeting point-of-sale. The sale opened a few weeks ago, so we don't know yet how many people bought it or use it. We also see that bad guys steal the work of each other and try to sell malware developed by other developers at a higher price. The final word will be a quote from Edbitts on a DiamondFox screenshot published by himself "In the future, even bank robbers will be replaced."**

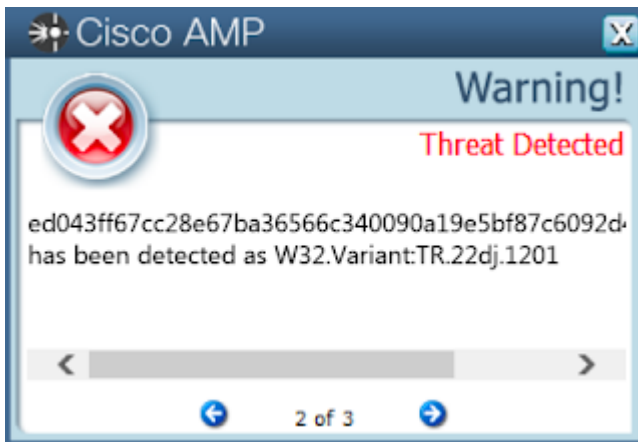


## Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✓
CloudLock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

[Advanced Malware Protection\(AMP\)](#) is ideally suited to prevent the execution of the malware used by these threat actors. Below is a screenshot showing how AMP can protect customers from this threat. Try AMP for free [here](#).



Cisco Cloud Web Security ([CWS](#)) or [Web Security Appliance \(WSA\)](#) web scanning prevents access to malicious websites and detects malware used in these attacks.

[Email Security](#) can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as [Next-Generation Firewall \(NGFW\)](#), [Next-Generation Intrusion Prevention System \(NGIPS\)](#), and [Meraki MX](#) can detect malicious activity associated with this threat.

[AMP Threat Grid](#) helps identify malicious binaries and build protection into all Cisco Security products.

[Umbrella](#), our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source SNORT® Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#).

## Indicators of Compromise (IOCs)

**The following IOCs are associated to this campaign:**

**GlitchPOS samples ed043ff67cc28e67ba36566c340090a19e5bf87c6092d418ff0fd3759fb661ab (SHA256)**

**abfadb6686459f69a92ede367a2713fc2a1289ebe0c8596964682e4334cee553 (SHA256)**

**C2 server coupondemo[.]dynamicinnovation[.]net**

**URLshxxp://coupondemo[.]dynamicinnovation[.]net/cgl-bin/gate.php**

**hxxp://coupondemo[.]dynamicinnovation[.]net/admin/gate.php**

**hxxp://coupondemo[.]dynamicinnovation[.]net/glitch/gate.php**