

GlitchPOS: New PoS malware for sale

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

The word "Glitch" is written in a bold, white, sans-serif font. Each letter has a red outline on the top and left sides, and a cyan outline on the bottom and right sides, creating a 3D, glitched effect. The text is set against a solid black background.The word "Glitch" is written in a bold, white, sans-serif font. Each letter has a red outline on the top and left sides, and a cyan outline on the bottom and right sides, creating a 3D, glitched effect. The text is set against a solid black background.

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

Executive summary

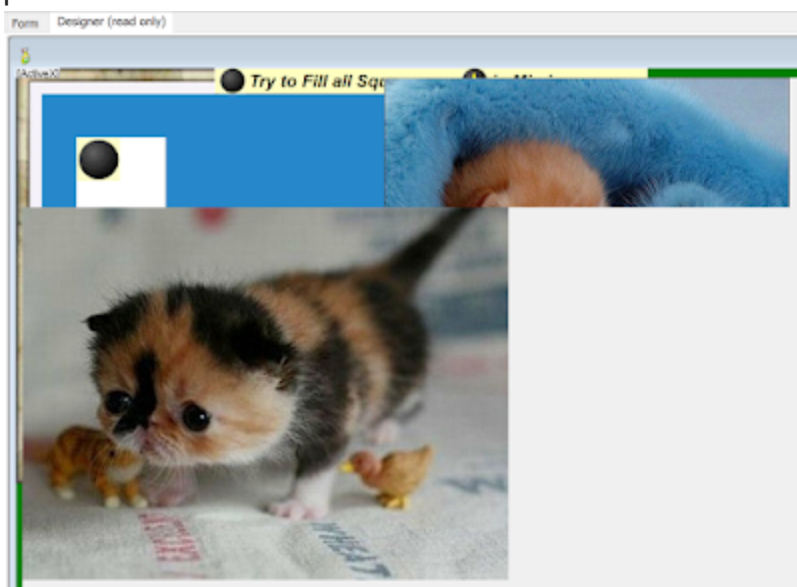
Point-of-sale malware is popular among attackers, as it usually leads to them obtaining credit card numbers and immediately use that information for financial gain. This type of malware is generally deployed on retailers' websites and retail point-of-sale locations with the goal of tracking customers' 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 LINK 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


```

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:

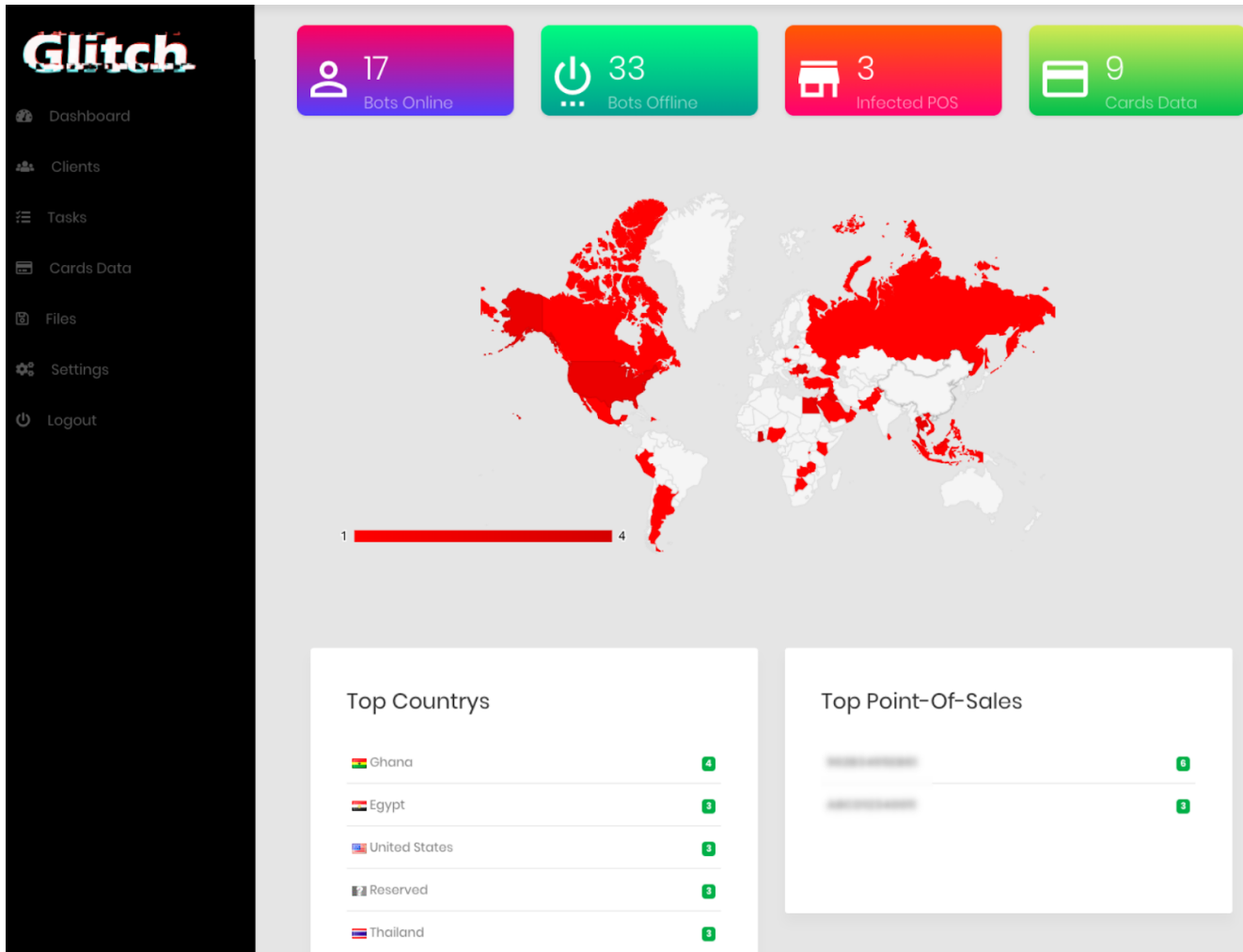
```
;\d{13,19}=\d{7}\w*\?  
;1234567890123445=99011200XXX00000000?*
```

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.

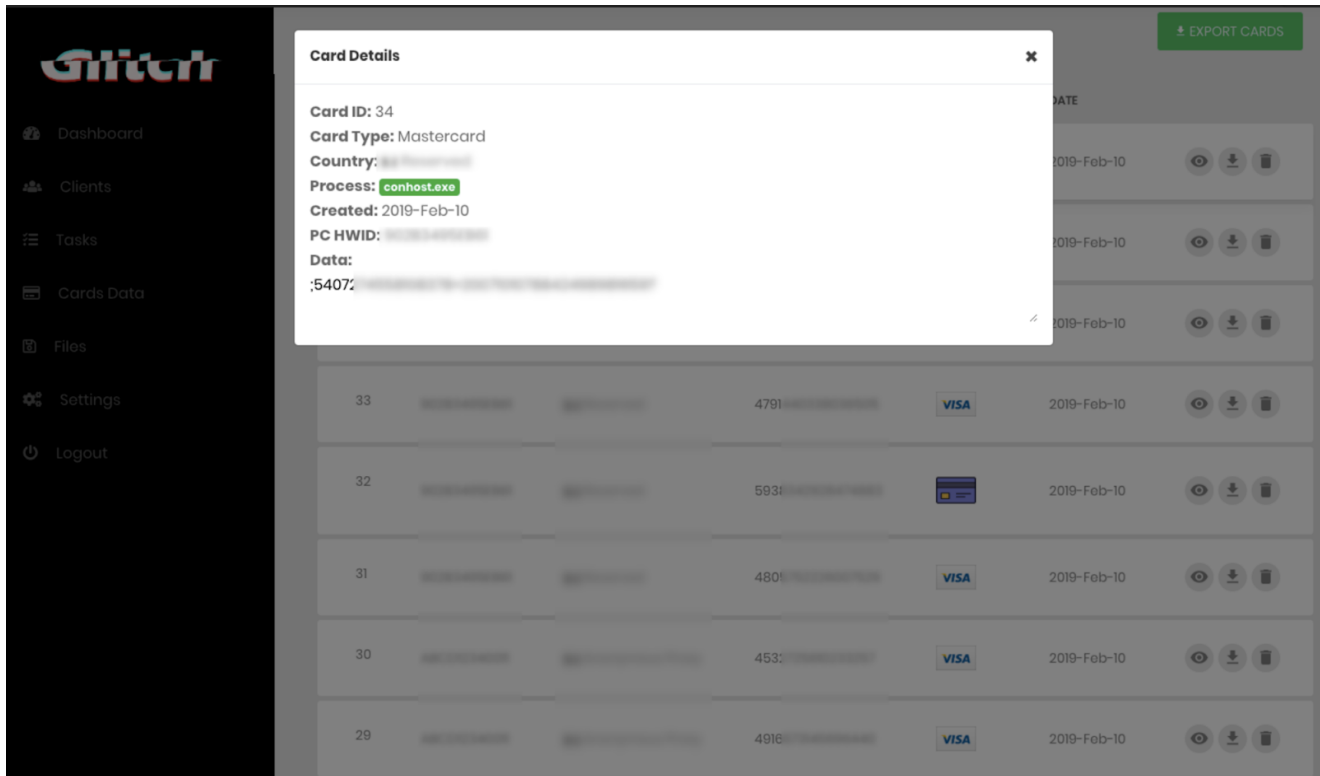
The "Dashboard:"



The "Clients" list:

HWID	IP	Country	PC-NAME	Cards	Status
XXXXXXXXXX	192.168.1.100	France	XXXXXXXXXX-PC	3	Offline
XXXXXXXXXX	192.168.1.101	France	XXXX-PC	3	Offline
XXXXXXXXXX	192.168.1.102	Czech Republic	JOHN-PC	0	Offline
XXXXXXXXXX	192.168.1.103	Thailand	DESKTOP-Q7RTRPG	0	Offline
XXXXXXXXXX	192.168.1.104	Malaysia	QX-PC	0	Online
XXXXXXXXXX	192.168.1.105	Kenya	HQICTDWK02379	0	Offline
XXXXXXXXXX	192.168.1.106	Ghana	DESKTOP-1PLEKSO	0	Offline
XXXXXXXXXX	192.168.1.107	Egypt	MAGIC-PC	0	Online
XXXXXXXXXX	192.168.1.108	Canada	TENEISHA-PC	0	Online

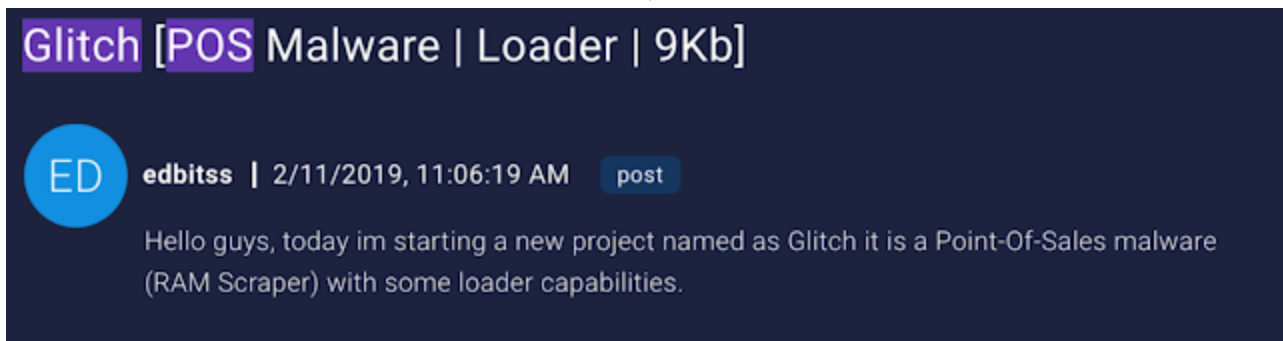
The "Cards Date:"



Linked with DiamondFox L!NK botnet


Author: Edbitss

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



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

edbits
Lurker
UID: 1330893



MEMBER

OFFLINE

Information

Username Changes: 0

Joined: 08-01-18


Date of Birth: Age Unknown - Birthday Unknown

Last Visit: Jan 16 2018 05:55 PM

Profile Views: 90

edbits

Vendor Of DiamondFox




Posts: 39
Joined: Apr 2016
Reputation: 3

Jabber: edbits@blah.im

Statistics

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

edbits Signature



Hello guys, im really happy to start a sales thread of the new DiamondFox version: Post: #1

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:

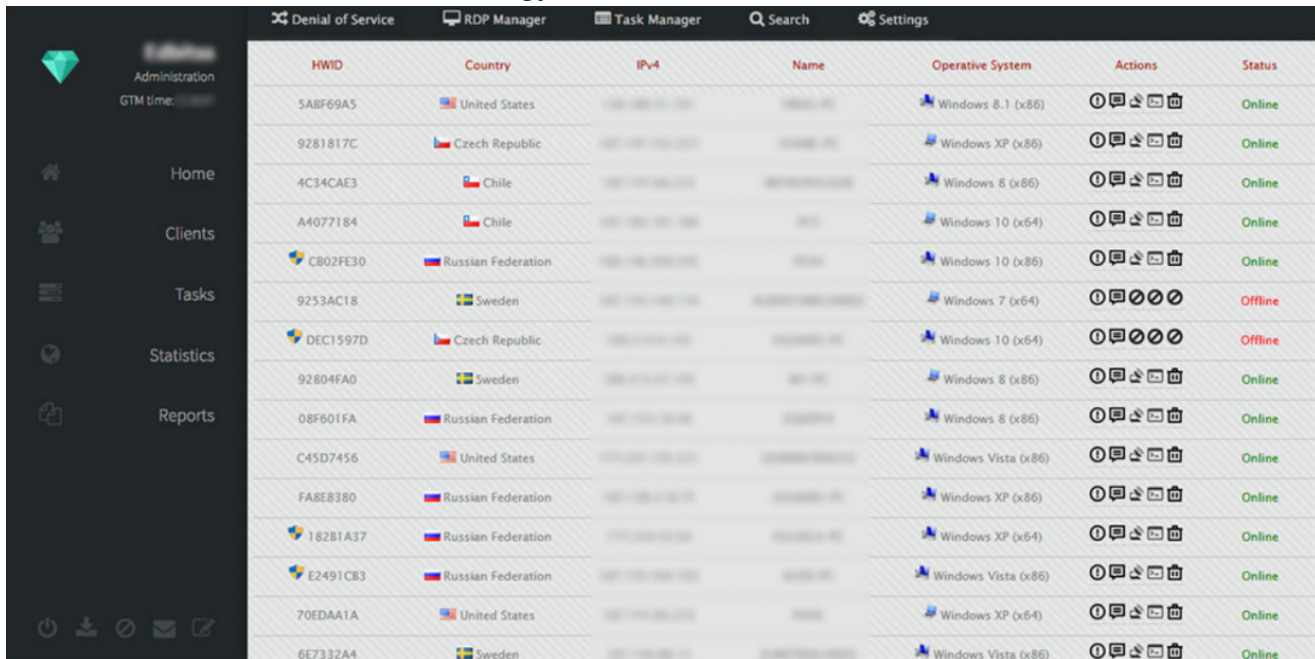
- Fully realtime (AJAX/JS) showing the last action/report sent or received for the bot.
- Extra security added: antforce, captcha and ban suspicious queries.
- The web panel can be hosted on windows servers without any kind of error.
- All communication with the panel are encrypted with a custom algorithm.

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).
- Persistence (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 author used the same terminology such as "Clients" or "Tasks" on the left menu:



HWID	Country	IPv4	Name	Operative System	Actions	Status
5ABF69A5	United States			Windows 8.1 (x86)	🔍 🗨 📄 🗑	Online
9281817C	Czech Republic			Windows XP (x86)	🔍 🗨 📄 🗑	Online
4C34CAE3	Chile			Windows 8 (x86)	🔍 🗨 📄 🗑	Online
A4077184	Chile			Windows 10 (x64)	🔍 🗨 📄 🗑	Online
CB02FE30	Russian Federation			Windows 10 (x86)	🔍 🗨 📄 🗑	Online
9253AC18	Sweden			Windows 7 (x64)	🔍 🗨 🚫 🚫 🚫	Offline
DEC1597D	Czech Republic			Windows 10 (x64)	🔍 🗨 🚫 🚫 🚫	Offline
92804FA0	Sweden			Windows 8 (x86)	🔍 🗨 📄 🗑	Online
08F601FA	Russian Federation			Windows 8 (x86)	🔍 🗨 📄 🗑	Online
C45D7456	United States			Windows Vista (x86)	🔍 🗨 📄 🗑	Online
FA8E8380	Russian Federation			Windows XP (x86)	🔍 🗨 📄 🗑	Online
182B1A37	Russian Federation			Windows XP (x64)	🔍 🗨 📄 🗑	Online
E2491CB3	Russian Federation			Windows Vista (x86)	🔍 🗨 📄 🗑	Online
70EDAA1A	United States			Windows XP (x64)	🔍 🗨 📄 🗑	Online
6E7332A4	Sweden			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 edbits on an alternative forum:

02-27-2019, 03:44 AM

GLITCH POINT OF SALE MALWARE



chameleon101 •

New Member



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

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).

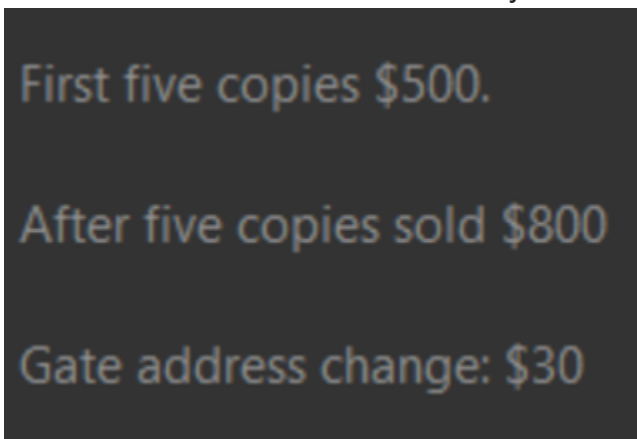
File melted after execution.

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

Panel:

Dashboard:

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



Some members even attempted to call out the unscrupulous behaviour:

02-27-2019, 03:47 AM

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

C3r34IK1ll3r •
New Member

Posts: 61
Threads: 3
B Rating: 0 1
Bytes: 52.6

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."

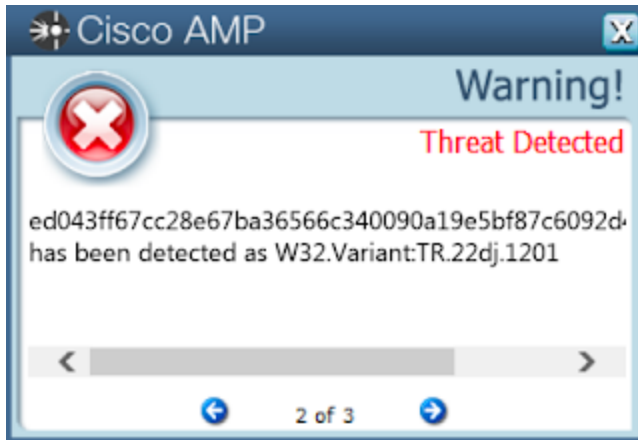


Coverage

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)
abfad6686459f69a92ede367a2713fc2a1289ebe0c8596964682e4334cee553 (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