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

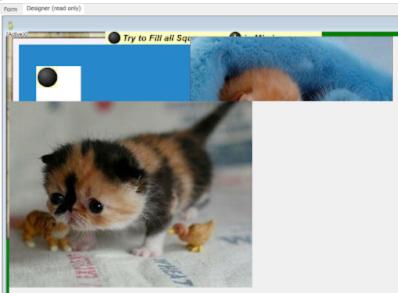
Point-of-sale malware is popular among attackers, as it usually leads to them obtaining credit card numbers and immediately use that information for financial gain. This type of malware is generally deployed on retailers' websites and retail point-of-sale locations with the goal of tracking customers'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

| Glitch | Create Task | | | | |
|------------------|-----------------|---|--|--|--|
| Gintern | File: | Parcourir Aucun fichier sélectionné. | | | |
| Dashboard | HWID filter: | <pre><hwid>, <hwid>,</hwid></hwid></pre> | | | |
| allents | | Example: 041127F5CE58,103028A8BE4D,184927F2AF5C | | | |
| Æ Tasks | Country filter: | ^ | | | |
| 🖃 Cards Data | | v | | | |
| 🕲 Files | Select a task: | Download & Execute (Memory) | | | |
| 📽 Settings | Task Type: | Downbad & Execute (Memory) Downbad & Execute (Disk) Uddate Uddate | | | |
| ப் Logout | Task status: | Unistal | | | |
| | • Add Task | | | | |

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

000000000000000005B8BFC6A42E8BB0300008B54242889118B54242C6A3EE8AA03000089116A4AE8A103000089396A1E6A3CE89D0300006A2268F4000000E8910300006A266A24E888 0300006A2A6A40E87F0300006A2E6A0CE8760300006A3268C800000E86A0300006A2AE85C0300008B09C70144000006A12E84D030000685BE814CF51E8790300006A3EE83B0300008BD 16A1EE8320300006A40FF32FF31FFD06A12E823030000685BE814CF51E84F0300006A1EE8110300008B098B513C6A3EE8050300008B3903FA6A22E8FA0200008B0968F80000005751FFD0 6A00E8E80200006888FEB31651E8140300006A2EE8D60200008B396A2AE8CD0200008B116A42E8C402000057526A006A006A046A006A006A006F31FFD06A12E8A902000068D03710F 251E8D50200006A22E8970200008B116A2EE88E0200008B09FF7234FF31FFD06A00E87E020000689C951A6E51E8AA0200006A22E86C0200008B118B396A2EE8610200008B096A40680030 0000FF7250FF7734FF31FFD06A36E8470200008BD16A22E83E0200008B396A3EE8350200008B316A22E82C0200008B016A2EE8230200008B0952FF775456FF7034FF316A00E8100200006 8A16A3DD851E83C02000083C40CFFD06A12E8F9010000685BE814CF51E8250200006A22E8E70100008B1183C2066A3AE8DB0100006A025251FFD06A36E8CE0100000C7010000000B82800 00006A36E8BC010000F7216A1EE8B30100008B118B523C81C2F800000003D6A3EE89F01000003116A26E8960100006A2852FF316A12E88A010000685BE814CF51E8B601000083C40CFFD 06A26E8730100008B398B098B71146A3EE86501000003316A26E85C0100008B098B510C6A22E8500100008B090351346A46E8440100008BC16A2EE83B0100008B0950FF77105652FF316A 00E82A01000068A16A3DD851E85601000083C40CFFD06A36E8130100008B1183C20189116A3AE8050100008B093BCA0F8533FFFFF6A32E8F40000008B09C701070001006A00E8E500000 068D2C7A76851E8110100006A32E8D30000008B116A2EE8CA0000008B0952FF7104FFD06A22E8BB000008B3983C7346A32E8AF0000008B318BB6A400000083C6086A2EE89D0000008B11 6A46E894000000516A045756FF326A00E88600000068A16A3DD851E8B200000083C40CFFD06A22E86F0000008B098B51280351346A32E8600000008B0981C1B000000089116A00E84F000 00068D3C7A7E851E87B0000006A32E83D0000008BD16A2EE8340000008B09FF32FF7104FFD06A00E8240000068883F4A9E51E850000006A2EE8120000008B09FF7104FFD06A4AE80400 00008B2161C38BCB034C2404C36A00E8F2FFFFF6854CAAF9151E81E0000006A406800100000FF7424186A00FFD0FF742414E8CFFFFFF890183C410C3E8220000068A44E0EEC50E84B0 0000083C408FF742404FFD0FF74240850E83800000083C408C355525153565733C0648B70308B760C8B761C8B6E088B7E208B3638471875F3803F6B7407803F4B7402EBE78BC55F5E5B59 5A5DC3555251535657886C241C85ED74438B453C8B54287803D58B4A188B5A2003DDE330498B348B03F533FF33C0FCAC84C07407C1CF0D03F8EBF43B7C242075E18B5A2403DD668B0C48B

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

| call | sub 419 | | |
|------|-----------------|----|----------------------|
| nush | 16B3FE88h | τ. | CreateProcessW |
| push | | 1 | er euterr occoon |
| | ResolveHash | | |
| | 2Eh ; '.' | | |
| | sub_419 | | |
| | edi, [ecx] | | |
| | 2Ah ; '*' | | |
| | | | |
| | sub_419 | | |
| | edx, [ecx] | | |
| | 42h ; 'B' | | |
| | sub_419 | | |
| push | | | |
| 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_40439E: var_A8(var_B4) = var_A8(var_B8) loc_4043E: var_A8(var_B4) = 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_403522: 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.

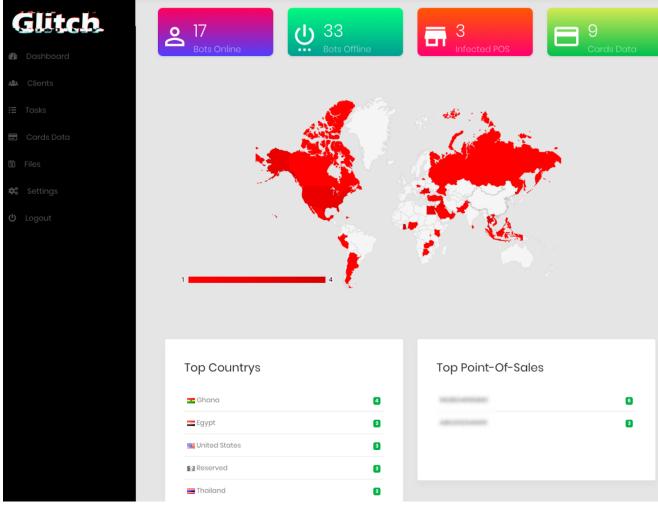
;\d{13,19}=\d{7}\w*\? The purpose of this regular expression is to detect Track 2 Here is an example of Track 2 based on the previous example: ;1234567890123445=99011200XXXX00000000?*

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:

| Glitch. | HWID | IP | Country | PC-NAME | Cards | Status |
|------------------|--------------|---------------|--|-----------------|-------|---------|
| Sucou- | 81283405030 | 86.220.76.82 | 84 ⁻¹ | | 6 | Offline |
| 🙆 Dashboard | ABC01034008 | | Aug. (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) | | 3 | Offline |
| 🖴 Clients | SADECCESSO | | Czech Republic | JOHN-PC | 0 | Offline |
| ≅ Tasks | 00000044028 | 10-42127.205 | Thailand | DESKTOP-Q7RTRPG | 0 | Offline |
| 🖬 Cards Data | THEADAICUESE | | 🖼 Malaysia | QX-PC | 0 | Online |
| | 007022402546 | 41212.22.76 | 🚘 Kenya | HQICTDWK02379 | 0 | Offline |
| පී Files | 304007048073 | 41,210,10,107 | 🚾 Ghana | DESKTOP-IPLEKSO | 0 | Offline |
| 🗱 Settings | 00808274C3A | 104.22140.223 | Egypt | MAGIC-PC | 0 | Online |
| ப் Logout | 180018713070 | 24.00714.40 | 🛃 Canada | TENEISHA-PC | 0 | Online |

The "Cards Date:"

| Gilitett | Card Details | | | | × | ± EXPORT CARDS |
|---|---------------------------------------|-----------|------|------|---------------------|----------------|
| | Card ID: 34 | | | | DATE | |
| DashboardClients | Card Type: Country: Process: co | nhost.exe | | | 2019-Fe | b-10 💿 主 🚺 |
| Æ Tasks | Created: 20 PC HWID: Data: | | | | 2019-Fe | b-10 💿 🛓 🔳 |
| Cards Data Files | ;54072 | | | | ² 019-Fe | b-10 💿 🖢 🔳 |
| 🈂 Settings | 33 | | 4791 | VISA | 2019-Fe | b-10 💿 🛃 🔳 |
| ப் Logout | 32 | | 593 | | 2019-Fe | b-10 💿 生 🔳 |
| | 31 | | 480 | VISA | 2019-Fe | b-10 • ± 1 |
| | | | 453: | VISA | 2019-Fe | b-10 • 🛃 |
| | 29 | | 4916 | VISA | 2019-Fe | b-10 • 🛃 |

Linked with DiamondFox L!NK botnet

Author: Edbitss

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



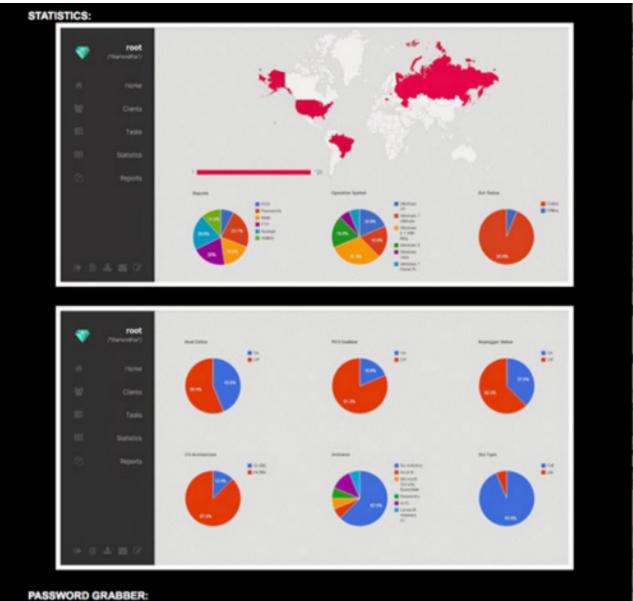
Edbitss is allegedly the developer of the DiamondFox L!NK botnet in 2015/2016 and 2017 as explained in a report by <u>CheckPoint</u>.

| edbitss Lurker U | ID: 1330893 | | | | |
|--|--|---|--|--|---|
| | A | Statistics | | | |
| , , | | Posts: | 0 (Find All Posts) | 🗪 Threads: | 0 (Find All Threads) |
| | | Leecher Value: | Neutral | \$ Credits: | 0 |
| 0 | | 🕀 Likes: | | Ye Vouches: | placeholder |
| | MEMBER | Reputation: | 0 | Trust Scan: | Info |
| < | IFFLINE | Warning level: | | Reported posts: | 0 |
| Information | | edbitss Signature | | | |
| Username Changes: | | | | | |
| Joined: | 08-01-18 | | | | |
| Date of Birth: | | Dia | mondFox | | |
| Last Visit: | Jan 16 2018 05:55 PM | | | | |
| Profile Views: | 90 | | | | |
| edbitss a Vendor Of DiamondFox | Hello guys, im really happy Panel: Spoiler (Click to View) Builder: | to start a sales thread of the | new DiamondFox version: | | Postr #1 |
| | Spoiler (Click to View) | | | | |
| Posts: 39 Joined: Apr 2016 Reputation: 3 | *Some information was blurred caus | e this address still in use for a campa | lgn. | | |
| Jabber: edbitss@blah.im | Loader: | | | | |
| | New cryptographic me | olility (x86 and x64 from XP to thods. ies (Bypass AVs proactives). |) Windows 10). | | |
| | Panel: | | | | |
| | Extra security added: The web panel can be | S) showing the last action/re; antiforce, captcha and ban su hosted on windows servers w the panel are encrypted with | uspicious querys. vithout any kind of error. | e bot. | |
| | Plugins: | | | | |
| | FTP Stealer (Filezilla). DDoS (UDP, Layer7 [3 Keylogger (Keyboard Email grabber (Outloo Live Mail, IncrediMail, RDP/VNC recover (Will) RAM Scrapper (Track2 Instant Messenger Gra GAIM/Pidgin, PaltalkS Screenshots (Single, E Spam (Custom SMTP, DNS Redirects (Remol) Persistance (Protect fi Crypto Wallet Stealer | Hook, HTML Report, Clipboard k Express, Microsoft Outlook Eudora, Netscape, Thunderb ndows RDP, TightVNC, Ultrav baber (Yahoo Messenger, Goo cene, Digsby). Each 30 seconds). html letter, unlimited email I | d Watcher, Get Window Titk 2000 [POP3 and SMTP], Mi ird, Yahoo! Mail, Hotmail/M: NC). ogle Talk, ICQ Lite 4.x/5.x/ ist). digital, Electrum-LTC, Multil | e, Get Time, Can be triggere crosoft Outlook 2002 to 2016 SN mall, Gmall). 2003, AOL Instant Messenger Doge, BitcoinDark, Unobtank | 5, Windows Mail, Windows r, Trillian, Miranda, um, Dash, Bitcoln, Litecoin, |

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):

| | | 1980 | . Bee | · · · | Actions |
|----|---|---------------|----------|--|--------------|
| - | root | PWS & ACP118D | 15.10.40 | Lungh Doore | |
| ×. | (Senandrar) | PW APCORCO | 12.00 40 | C Representation of the second state of the | |
| | 100000000000000000000000000000000000000 | Priv ESICENTE | 12.87 kb | OR. 1 https://accounts.google.com/tarvio | elagistath 2 |
| | 1000 | PW-RESCRIPTE | 12.94.40 | ant Branat I Origan | |
| | 10me | PVII ADDADBAB | 14.6840 | Partnerd - Strength - Streng | |
| | 1000 | PW 8-4900140 | 16.2 10 | Duer Name Field : Small Parameter Field : Paramet | |
| | Cleris | Priv assegmed | 14.0710 | | |

| | | Contract Con | RDP Manager | Task Manager | Q Search | Ø 8 Settings | | |
|---|----------------|--|--------------------|--------------|----------|-----------------------|---------|---------|
| - | Administration | HWID | Country | IPv4 | Name | Operative System | Actions | Status |
| | GTM time: | SABF69A5 | 🔜 United States | | | 💐 Windows 8.1 (x86) | ◑▣◈▫◧ | Online |
| | | 9281817C | 🖿 Czech Republic | | | 🚚 Windows XP (x86) | ◑▣◈▫◧ | Online |
| | Home | 4C34CAE3 | 🏪 Chile | | | 👋 Windows 8 (x86) | ◑▣๙⊵₫ | Online |
| | Clients | A4077184 | 🔚 Chile | | | June 20 (x64) | ⓓ▣⋞⋻⋣ | Online |
| | | CB02FE30 | Russian Federation | | | 💐 Windows 10 (x86) | ◑▣◈▫◧ | Online |
| | Tasks | 9253AC18 | 🔚 Sweden | | | 🗸 Windows 7 (x64) | 00000 | Offline |
| | Statistics | 🐓 DEC1597D | 🖿 Czech Republic | | | 💐 Windows 10 (x64) | 00000 | Offline |
| | Statistics | 92804FA0 | Sweden | | | 🖊 Windows 8 (x86) | ◑▣◈▫◧ | Online |
| | Reports | 08F601FA | Russian Federation | | | 🦄 Windows 8 (x86) | ◑▣◈▫◧ | Online |
| | | C45D7456 | 🔜 United States | | | 🂐 Windows Vista (x86) | ⓓ▣⋞⊵₫ | Online |
| | | FA8E8380 | Russian Federation | | | 💐 Windows XP (x86) | ᠿ፼ዸ⊵⊡₫ | Online |
| | | 💙 18281A37 | Russian Federation | | | 💐 Windows XP (x64) | ◑▣ඵ▣◧ | Online |
| | | 💙 E2491CB3 | Russian Federation | | | 🦂 Windows Vista (x86) | ◑▣◈▫◧ | Online |
| | 0 2 2 | 70EDAA1A | 🖼 United States | | | 🚚 Windows XP (x64) | ◑▣๙▻◧ | Online |
| | | 6E7332A4 | Sweden | | | Windows Vista (x86) | 00200 | Online |

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

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

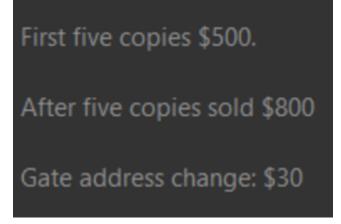
In 2017, the DiamondFox malware included a POS plugin. We decided to check if this module was the same as GlitchPOS, but it is not. For DiamondFox, the author decided to use the leaked code of BlackPOS to build the credit card grabber. On GlitchPOS, the author developed its own code to perform this task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

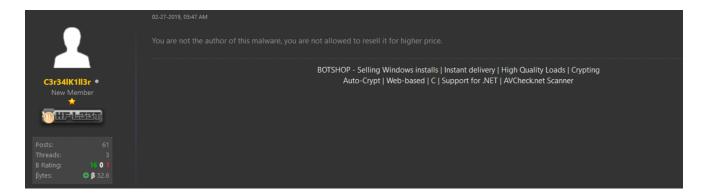
| GLITCH POS MALWARE LOADER | 9KD | |
|-------------------------------|---|------------------------------|
| | 02-27-2019, 03:44 AM | |
| | Hello friends | GLITCH POINT OF SALE MALWARE |
| | I bring to your attention "GLITCH" a professional pos malware. | |
| HF | FEATURES: | |
| chameleon101 • | File size: 9kb (10kb with configurations). | |
| New Member | Grab Track1 and Track2 Data. | |
| | No dependencies. | |
| | Persistence (persists in pos terminal for a long time) | |
| Threads: 4 B Rating: 0 0 | File tested from XP to W10 (x86 and x64). | |
| βytes: 🔮 🛱 570.8 | Communication between loader and panel are encrypted. | |
| | Configurations encrypted and mixed inside the loader. | |
| | | |
| | 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) | |
| | | |
| | Dashboard: | |

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



CUTCUL DOG MAUWART LLO

Some members even attempted to call out the unscrupulous behaviour:

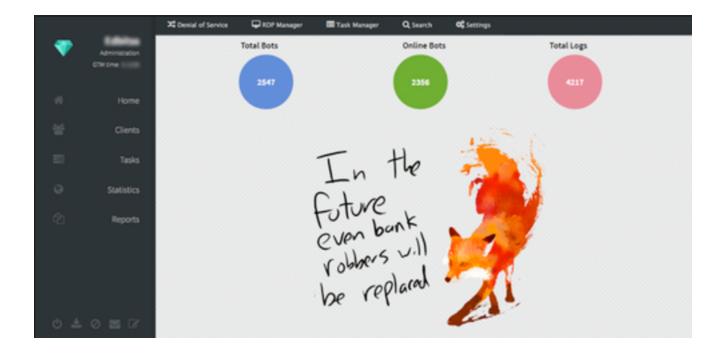


With the different information we have, we think that Chameleon101 has taken the previous malware created by Edbitss to sell it on an alternative forum and with a higher price.



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 | v |
| CloudLock | N/A |
| cws | v |
| Email Security | v |
| Network Security | v |
| Threat Grid | * |
| Umbrella | v |
| WSA | ~ |

<u>Advanced Malware Protection</u> (<u>AMP</u>) 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 <u>here</u>.



Cisco Cloud Web Security (<u>CWS</u>) or<u>Web Security Appliance (WSA</u>) 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<u>Next-Generation Firewall (NGFW), Next-Generation</u> <u>Intrusion Prevention System (NGIPS)</u>, and <u>Meraki MX</u> can detect malicious activity associated with this threat.

<u>AMP Threat Grid</u> helps identify malicious binaries and build protection into all Cisco Security products.

<u>Umbrella</u>, 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 <u>Snort.org</u>.

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/cgl-bin/gate.php hxxp://coupondemo[.]dynamicinnovation[.]net/admin/gate.php hxxp://coupondemo[.]dynamicinnovation[.]net/glitch/gate.php