

# GratefulPOS credit card stealing malware - just in time for the shopping season

community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

December 8, 2017

**RSA FirstWatch would like to thank the Target Cyber Threat Intelligence & Detection Team for sharing technical insight into the topic of this post.**

Well into the holiday season, people are making their shopping lists, recovering from Black Friday and Cyber Monday, and perhaps contemplating the many things for which they are grateful. Criminals, too, are making their lists, and posturing for the big shopping days ahead.

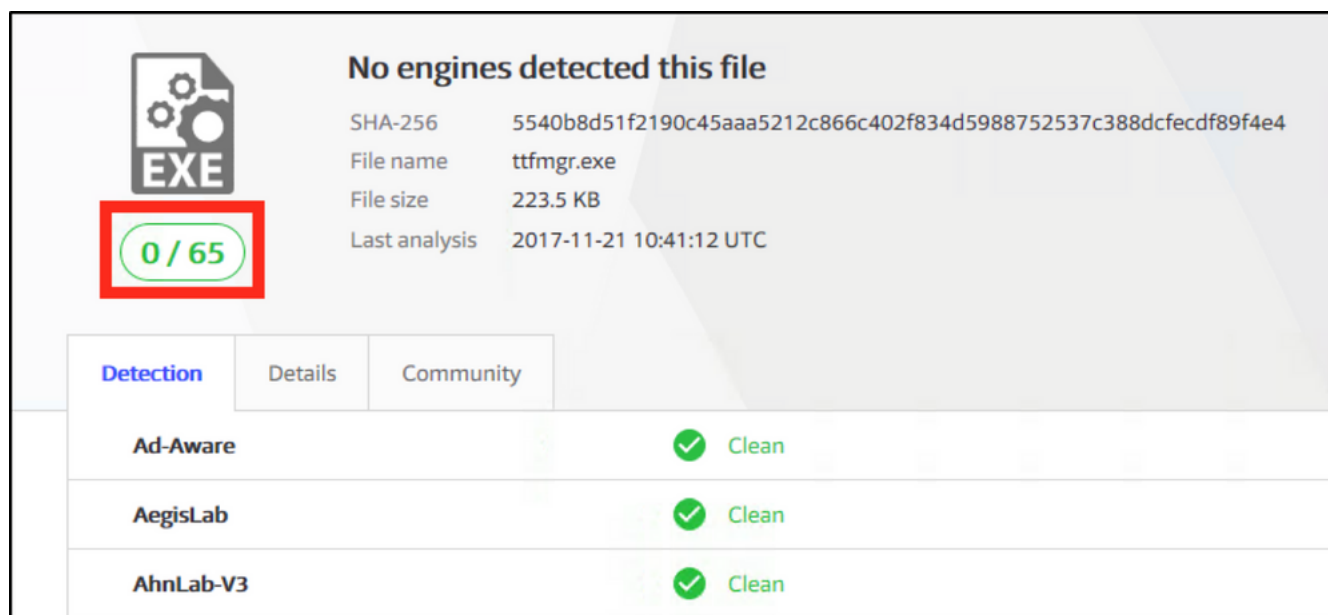
Threat researchers are still at work of course, so it was inevitable that FirstWatch contemplated which things credit card stealing criminals--AKA "carders" appreciate. This is what we came up with.

## What carders are thankful for this year

1. Malicious code and techniques shared by other criminal developers
2. Merchants that still use swipe-only Point of Sale (POS) systems
3. Merchants with POS systems that lack Point-to-Point (P2P) encryption of payment card data
4. Merchants that employ antivirus easily bypassed by unsophisticated malware

With a combination of one or more of these carder's favorite things, intruders have stolen payment card data associated with millions of consumers (like us), resulting in tens of billions of dollars of losses annually.

We would like to illustrate a carder's favorite thing number four with a sample of malware uploaded to the VirusTotal website on Tuesday morning, 21 November 2017, **detected by zero out of 65 different antivirus** vendors (Figure 1).



The screenshot shows the VirusTotal interface for a file named 'ttfmgr.exe'. The file is identified as an EXE. The analysis results show 'No engines detected this file'. The file's SHA-256 hash is 5540b8d51f2190c45aaa5212c866c402f834d5988752537c388dcfecdf89f4e4. The file size is 223.5 KB, and the last analysis was performed on 2017-11-21 at 10:41:12 UTC. A red box highlights the '0 / 65' detection count. Below the main information, there are tabs for 'Detection', 'Details', and 'Community'. The 'Detection' tab is active, showing a list of antivirus engines and their results:

Engine	Result
Ad-Aware	Clean
AegisLab	Clean
AhnLab-V3	Clean

Figure 1 Zero detection POS RAM-scraping malware uploaded to VT

Certainly this won't be the last POS malware not detected (statically and initially, at least) by any antivirus, nor is it the first. Consider the analysis of the zero detection [Getmypass POS malware by Nick Hoffman](#) during the holiday season three years ago[i].

“While this isn't the most advanced POS RAM scraper there is, it's still capable of bypassing all 55 AV's used to scan it.”

Three years later, there are now ten more antivirus vendors represented on VirusTotal, whose static scans are still bypassed by this recent iteration of payment card information stealing malware.

By their very nature, merchant POS intrusions are rather targeted, and if the minimal barrier to installation of their payment card collector/exfiltrator is an antivirus, merchant intruders so far continue to effectively bypass that minimal barrier.

FirstWatch would like to use this post to expose this particular campaign that unfortunately has been active since at least February of this year, with indications that thousands of credit card numbers from targeted merchants are being exfiltrated to the perpetrators at this very moment. With any luck, we hope to make this perpetrator's holiday season perhaps a little less enjoyable than yours. Will use some of the tools at our

ready disposal, namely NetWitness and What's This File, to peer into its behavior.

This malware is a variant of FrameworkPOS, and shares some code with other POS malware families variously known as TRINITY, BlackPOS, and BrickPOS, so we have decided to call it GratefulPOS, because, well, tis the season.

## A set it and forget it stealer, not a controller

This is a tool designed to scrape and exfiltrate payment card information from one or more processes in use by a Windows-based Point of Sale system, from probably a wide variety of POS vendors. Compiled for x64 architectures, we can assume that this malware is designed to run on POS systems running Windows 7 or later. It has no command and controller capability itself; the perpetrator uses other means of privileged access to install and execute the malware on the target POS systems.

GratefulPOS has the following functions

1. Access arbitrary processes on the target POS system
2. Scrape track 1 and 2 payment card data from the process(es)
3. Exfiltrate the payment card data via lengthy encoded and obfuscated DNS queries to a hardcoded domain registered and controlled by the perpetrators, similar to that described by Paul Rascagneres in his analysis of FrameworkPOS in 2014 [iii], and more recently by Luis Mendieta of Anomoli in analysis of a precursor to this sample [iv].

## GratefulPOS WTF Score

A high threat score of 80 is computed when GratefulPOS is submitted to RSA What's This File (<https://whatsthisfile.rsa.com>, Figure2)

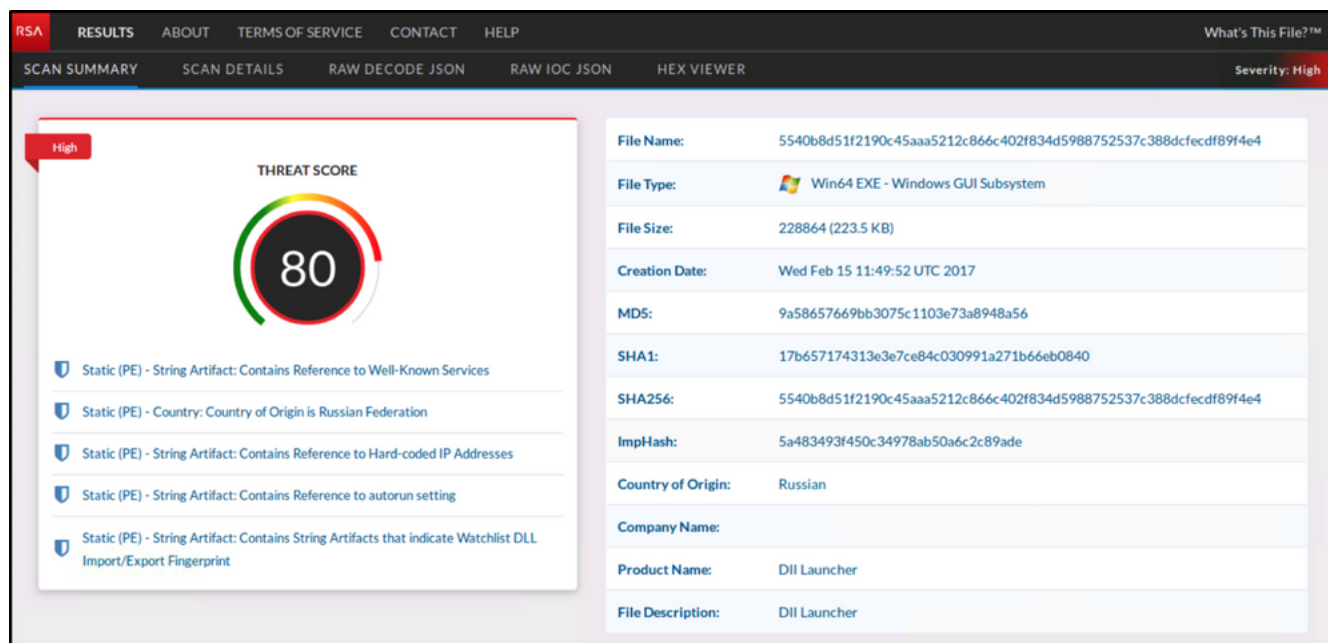


Figure 2 GratefulPOS scores a high 80 on WTF

## NetWitness Endpoint and GratefulPOS

The GratefulPOS sample was executed on a renamed but otherwise stock Windows x64 VM running NetWitness Endpoint, and analyzed through the NWE UI.

The malware installs itself as persistent Windows service, with a legitimate sounding name "TrueType Fonts Management Service" (Figure 3).

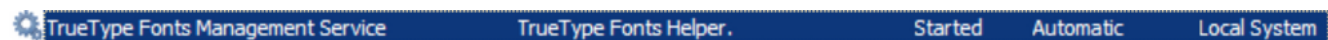


Figure 3 GratefulPOS Windows service

Combined risk and Instant Indicators of Compromise (IIOC) score rose significantly from 23 (Figure 4) to 159 (Figure 5) after the malware installation.



Figure 4 NetWitness Endpoint before GratefulPOS execution



Figure 5 NetWitness Endpoint score after GratefulPOS execution and installation

NWE reveals the process memory scraping activity typical of RAM-scraping POS malware, by tracking GratefulPOS's access to consecutive processes on the system in the Tracking panel (Figure 6).

Tracking			
Event Time	Source File Name	Event	Target
11/22/2017 12:28:04.961 PM	tffmgr.exe	Open Process	WmiApSrv.exe
11/22/2017 12:24:50.787 PM	tffmgr.exe	Open Process	more.com
11/22/2017 12:24:49.274 PM	tffmgr.exe	Open Process	TPAutoConnect.exe
11/22/2017 12:24:44.594 PM	tffmgr.exe	Open Process	TrustedInstaller.exe
11/22/2017 12:24:43.627 PM	tffmgr.exe	Open Process	cmd.exe
11/22/2017 12:24:41.942 PM	tffmgr.exe	Open Process	msdtc.exe
48 items total			

Figure 6 GratefulPOS process memory scraping observed in NWE tracking panel

### More credit card numbers, more DNS traffic

GratefulPOS has a simple and efficient method of exfiltrating scraped payment card data to the perpetrator by means of DNS queries to a malicious controlled domain and DNS name server daemon. This method can typically bypass firewall and other enclaving set up on a merchant's POS network infrastructure because the compromised POS system does not need to communicate directly to the Internet. It can just as easily communicate to an internal DNS server on the merchant's network, which would presumably pass on the payment card data encoded in the DNS queries, to the perpetrator.

We observed the initial DNS "check-in" beacon communication on our test system in NetWitness Packets, that sent information about the compromised system to the perpetrator.

Query

```
44105+ A? 93c61f10.v1702.ping.adm.cdd2e9cde8e8e9cde8e8e9fec4fc.fcfee9fec4c8e9cdc4cde9fefec4.c59dec87ed9dd8d8fa.ns.a193-108-94-56-deploy-akamaitechnologies.com. (166)
```

Response

```
44105 1/0/0 A 96.44.135.70 (182)
E...f...<4....
....5....w.l.....93c61f10.v1702.ping.adm.cdd2e9cde8e8e9cde8e8e9fec4fc.fcfee9fec4c8e9cdc4cde9fefec4.c59dec87ed9dd8d8fa.ns(a193-108-94-56-deploy-akamaitechnologies.com
```

Beacon communication was to a public DNS server (lower part of Figure 7), however, it could have been to an internal DNS server, further hiding its origins on a large enterprise network by the time it leaves the perimeter.

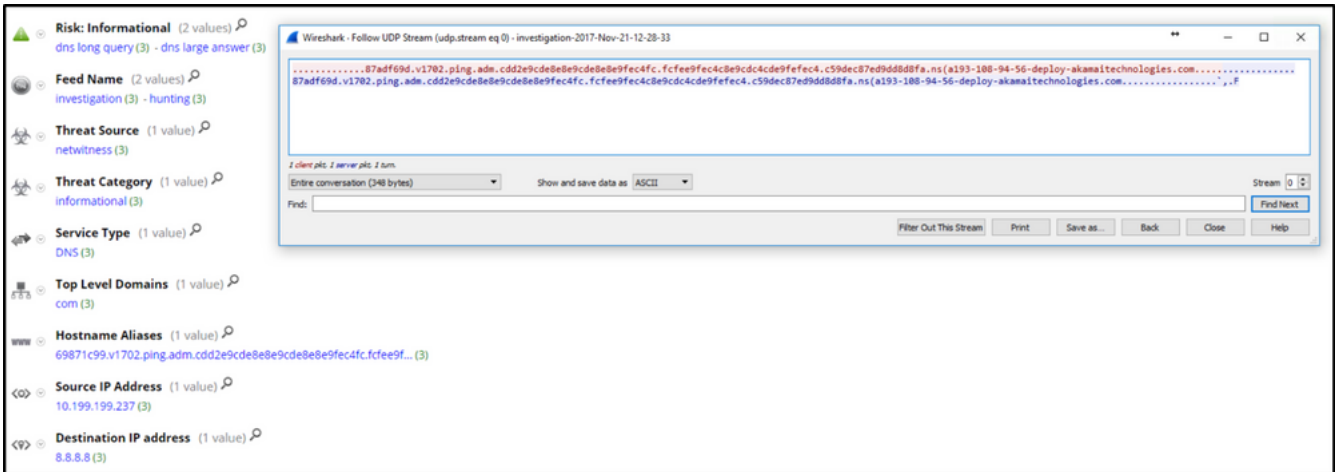


Figure 7 GratefulPOS malware initial DNS beacon communication to public DNS server

To add insult to injury, the domain was not selected at random. It was designed to mimic legitimate DNS queries typically encountered in volume on large enterprise networks, associated with the large Content Delivery Network (CDN) service Akamai. We have reached out to Akamai with this information.

We used NetWitness Packets to observe GratefulPOS perform a web check-in to the malicious name server on port 80. The web server responded with a page that displayed the compromised system's public IP address (Figure 8).

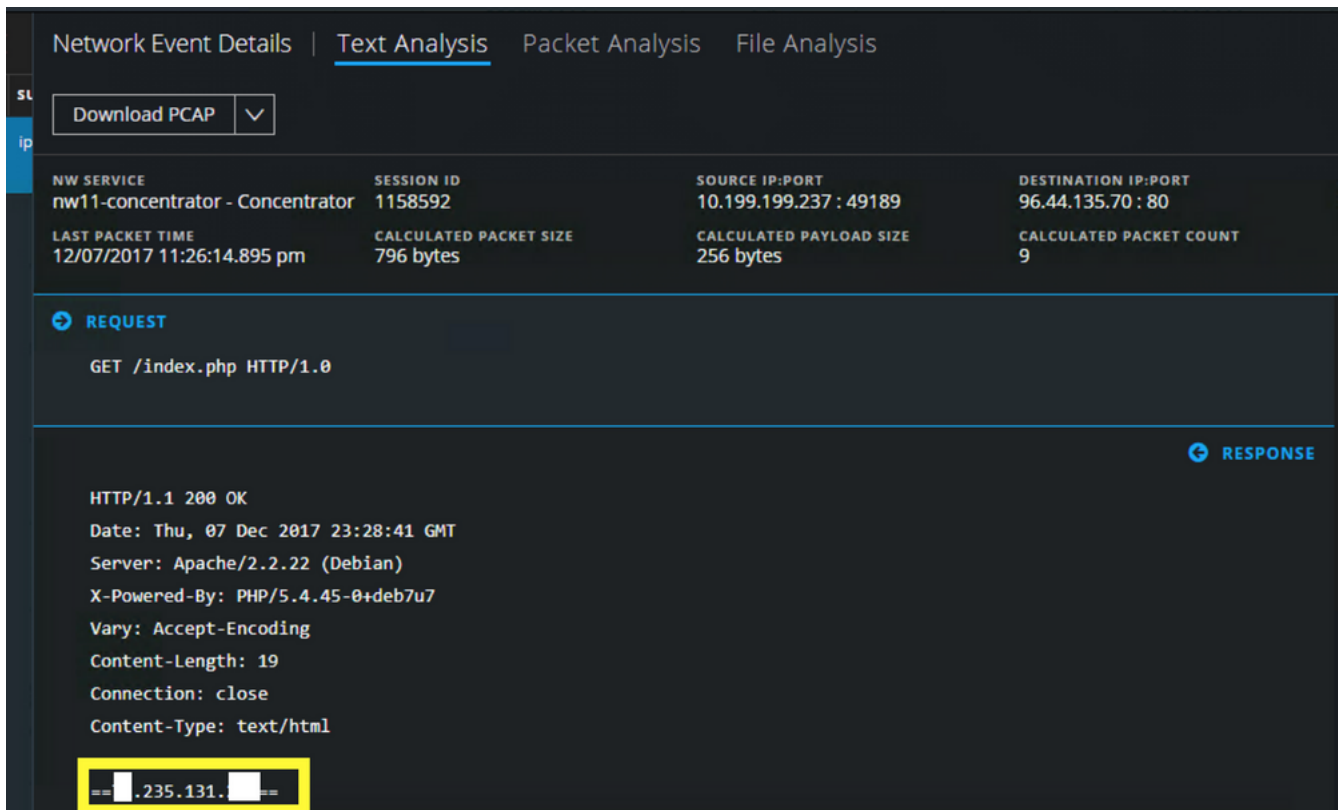


Figure 8 NetWitness 11 display of GratefulPOS malware web check-in with public IP response in body

It appears that the malware developer created their own IP information service, perhaps to help them organically track the source and public network infrastructure of their targeted POS systems, rather than using one of the many free services available such as ipinfo.io, ipchicken.com or canihazip.com.

We also generated a few hundred fake credit card numbers and formatted them as would be encountered on a real POS system, and observed via NetWitness as the payment card information flew out the door via encoded DNS to the still clearly active exfiltration node (Figure 9).

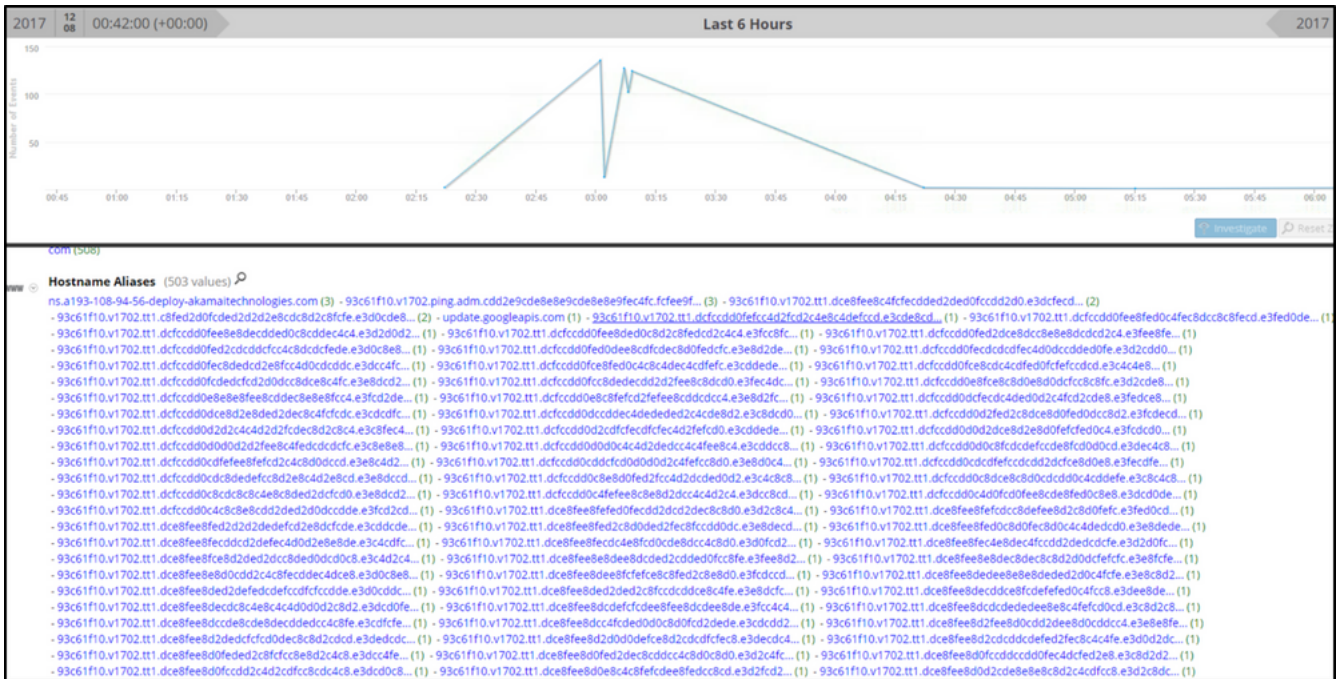


Figure 9 GratefulPOS exfiltrates credit card numbers as observed with NetWitness

Compared to the sample analyzed by Mr. Mendieta of Anomali in 2015, we observed only minor code changes. Instead of the particular campaign specified by “grp” strings, we see “v1702” is the campaign identifier, as displayed in an exfiltration packet (Figure 10).

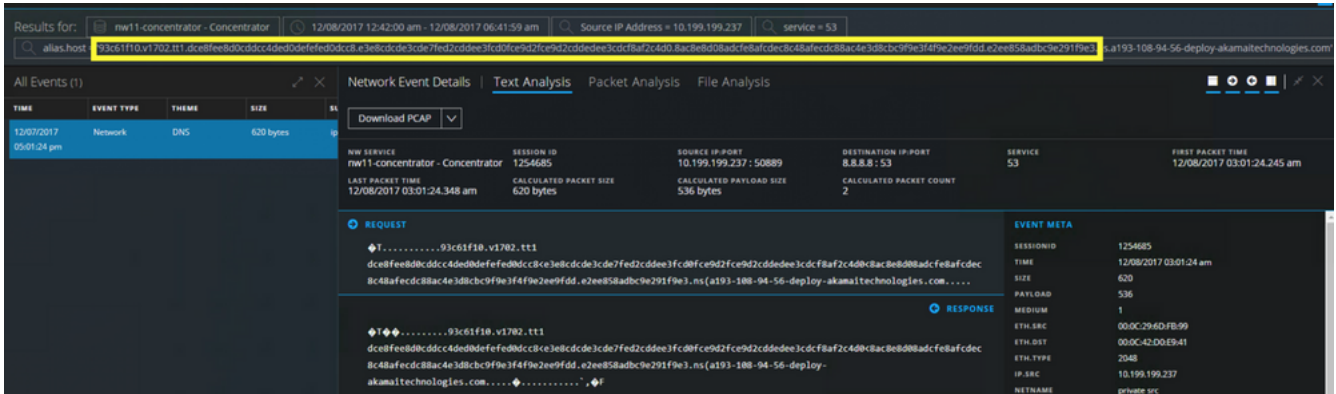


Figure 10 Encoded Track 1 data with campaign identifier “v1702” as observed in NetWitness 11 event analysis

## Implications and Conclusions

As Paul Rascagneres suggested, this DNS exfiltration method employed by the POS malware is clever. It effectively negates a common POS system control employed by payment card merchants, which is blocking direct access to the Internet from the POS systems. If the POS systems point to internal DNS servers, this malware should have no problem exfiltrating credit card data en masse without direct connect to the Internet.

Keen visibility of enterprise endpoints and network traffic allows an analyst to detect business and customer-critical threats not otherwise detected by antivirus. Hardware-enabled Point-to-Point encryption of payment card data would prevent RAM scrapers like FrameworkPOS and GratefulPOS from working at all. In absence of that, one strategy as mentioned by Mr. Rascagneres from GData includes DNS domain whitelisting of only necessary domains needed for POS function.

## Indicators of Compromise

The exfiltration domain and current exfiltration DNS server IP address have been added to the RSA FirstWatch C2 Domains and IPs feeds.

Table 1 GratefulPOS Indicators of Compromise

GratefulPOS MD5	9a586657669bb3075c1103e73a8948a56
-----------------	-----------------------------------

---

GratefulPOS exfiltration domain a193-108-94-56-deploy-akamaitechnologies.com

---

Current Exfiltration DNS server 96.44.135.70

## FirstWatch

---



<https://wallethub.com/edu/credit-debit-card-fraud-statistics/25725/>

[ii] <http://securitykitten.github.io/getmypass-point-of-sale-malware/>

[iii] <https://www.gdatasoftware.com/blog/2014/10/23942-new-frameworkpos-variant-exfiltrates-data-via-dns-requests>

[iv] <https://www.anomali.com/blog/three-month-frameworkpos-malware-campaign-nabs-43000-credits-cards-from-poi>