Visa Security Alert **JUNE 2019**

ALINA POINT-OF-SALE MALWARE CLASSIFICATIONS

Distribution: Visa Issuers, Processors and Acquirers

Summary

In June 2019, Visa's Payment Fraud Disruption (PFD) analyzed a malware sample from the recent compromise of a North American hospitality merchant and identified the malware as a variant of the Alina Point-of-Sale (POS) malware family. Alina dates back to at least 2013, and is one of many malware strains that possesses a Random Access Memory (RAM) scraper, which is specifically designed to steal payment account information from the memory, or RAM, of the targeted system.

Analysis on the malware sample from the aforementioned merchant breach led to the identification of additional malware samples recently uploaded to a popular open-source malware repository, which Visa assesses are all variants of the Alina POS malware family. The most recent uploads occurred in May 2019, however PFD identified numerous associated files that were uploaded throughout 2018. The variant observed in the recent merchant compromise is of the Domain Name Service (DNS) variant which uses DNS traffic for Command and Control (C2) operations. Given the upload and compile dates, and recently observed operations leveraging Alina, PFD assesses Alina POS is in active use and remains a popular malware variant for POS targeting.

Alina Classifications

Similarities between the identified malware samples (e.g. same signing certification, same imphash, similar themed C2 domains, etc.) led to the conclusion that the malware variants are all related and belong to the Alina POS family. Moreover, based on the C2 communication method utilized by the specific Alina POS malware samples, three distinct classifications of Alina were identified and dated based on their compile dates:

- **HTTPS/SSL Variant** – Used in 2017 and early 2018, these samples utilize Hypertext Transfer Protocol Secure (HTTPS)/Secure Socket Layer (SSL) for secure C2 communication
- **HTTPS/SSL & DNS Variant** – Used in April 2018, these samples utilize both HTTPS and DNS for C2 communication.
- **DNS Variant –** Used in late 2018 through 2019, these samples, which include the sample from the recent merchant breach, solely utilize DNS for C2 communication

Indicators of Compromise (IOC)

Related malware samples analyzed by PFD are detailed below and are broken into three different sections:

1. AlinaPOS - Section #1

The following malware samples share the **same C2 domain** (analytics-akadns[.]com) as the Alina POS (DNS Variant) malware used in the recent merchant breach. The observed processes and signing certificates of the malware samples are provided below, and the indicators of compromise are included in the corresponding CSV file.

Malware sample 1.1

Source	Virus Total
MD5	176633d74a4a93fe0a76d59175ce54bc
SHA1	02783a013d8d65e38c13dcc02f3e689e3c7f2c71
SHA256	0ae4740e74f7350adb13b23e5a2094b2821aafb49ec122a789b1e98ee93458fd
SSdeep	6144:s4wK3wVv8SoHhruKPKHLMvdkfmBEWZ+amiamQVi+s6RBzS:s4w1EpirGOfm0aEmF6RBzS
Imphash	02ee548fb82390bf382103b507873bbe
Note	Alina POS Malware - Deployment Loader
Sample	1.1

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 6:41 AM 4/11/2018
Certificate Common Name: GESO LTD
Certificate SHA-1 Thumbprint: 744160F36BA9B0B9277C6A71BF383F1898FD6D89
Certificate Serial Number: 00 B7 E0 CF 12 E4 AE 50 DD 64 3A 24 28 54 85 60 2F

Deployment

During execution, the loader deploys a variant of the Alina POS Malware into the "**D:\POS\AlohaQS**\" directory.

Malware sample 1.2

Compile Time: 2018-04-11 12:42:26

Source	Virus Total
MD5	b62b0a7907bec6f7dd0cc88854fbd407
SHA1	1f62704a9f9ea87d3f8dd0f296bd602294168632
SHA256	c0b4ab7a897102ceea5ce82a36018cb5d20806dd47db61484c4ea8e331a423c7
SSdeep	3072:oH+ywv9EfGdHLMHVZRVwO6PfMXoff6EWZ+xImimV3qraz4Wh1cwWf12WA5c+s692:+KHLMvdkfmBEWZ+amiamQVi+s6Q
Imphash	84bf21e06080a07068692a185e3de384
Note	Alina POS Malware (HTTPS/SSL & DNS Variant)
C2 - DNS Request(s)	analytics-akadns[.]com testttdomain
C2 - HTTP Request(s)	hxxps://testttdomain/wp-admin/gate1.php
Sample	1.2

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 6:41 AM 4/11/2018
Certificate Common Name: GESO LTD
Certificate SHA-1 Thumbprint: 744160F36BA9B0B9277C6A71BF383F1898FD6D89

Certificate Serial Number: 00 B7 E0 CF 12 E4 AE 50 DD 64 3A 24 28 54 85 60 2F

Service Installation

The loader executes the dropped variant of Alina POS Malware using the "install" command line option. The "install" option will choose 1 of 30 different hard-coded service profiles and register the Alina POS malware as a service along with a persistence registry key and location.

Self-Deletion

After installation of the Alina POS Malware, the loader pauses briefly (ping wait) and then deletes itself with the following command:

cmd.exe /c ping localhost -n 3 > nul & del "**<path_to_loader>**" & exit

Malware sample 1.3

Compile Time: 2018-04-11 12:42:26

Source	Virus Total
MD5	3b016d76fc60cc9c46da6fa10efd0315
SHA1	93c33ae5035bee6da2bf10784df1b8d32db416f9
SHA256	804559ea57381bd6c2301d0c9393cf3768e54455ece74acdb99bb307f80494eb
SSdeep	3072:oH+ywv9EfGdHLMHVZRVwO6PfMXoff6EWZ+xImimV3qraz4Wh1cwWf12WA5c+s69z:+KHLMvdkfmBEWZ+amiamQVi+s6R
Imphash	84bf21e06080a07068692a185e3de384
Note	Alina POS Malware (HTTPS/SSL & DNS Variant)
C2 - DNS Request(s)	analytics-akadns[.]com testttdomain
C2 - HTTP Request(s)	hxxps://testttdomain/wp-admin/gate1.php
Sample	1.3

Authenticode Signature Block

Signature verification: Signed file, valid signature
Signing Date: 4/11/2018
Certificate Common Name: GESO LTD
Certificate SHA-1 Thumbprint: 744160F36BA9B0B9277C6A71BF383F1898FD6D89
Certificate Serial Number: 00 B7 E0 CF 12 E4 AE 50 DD 64 3A 24 28 54 85 60 2F

Malware sample 1.4

Compile Time: 2018-04-11 11:58:38

Source	Virus Total
MD5	97a95075ec7dc0edac17864cb1ba5a5d
SHA1	985bff8d5a8346fc514048fd25920811f602adb0
SHA256	83e3df5ec961ce9b24588ba95025ce94e34c319a8afa30fab2b7cca10c0ef904
SSdeep	6144:L4wK3wVv8SoHhreeOKHLMvdkfmBEWZ+amiamwVi+s6oBzL:L4w1EpbrGOfm0aEml6oBz
Imphash	02ee548fb82390bf382103b507873bbe
Note	Alina POS Malware - Deployment Loader

Sample	1.4

Authenticode Signature Block

Signature verification: Signed file, valid signature
Signing Date: 5:57 AM 4/11/2018
Certificate Common Name: GESO LTD
Certificate SHA-1 Thumbprint: 744160F36BA9B0B9277C6A71BF383F1898FD6D89
Certificate Serial Number: 00 B7 E0 CF 12 E4 AE 50 DD 64 3A 24 28 54 85 60 2F

Deployment

During execution, the loader deploys a variant of the Alina POS Malware into the "**D:\POS\Aloha\**" directory.

Malware sample 1.5

Compile Time: 2018-04-11 11:58:35

Source	Virus Total
MD5	f49c6afd16afcc5507e0aa7acb64f06f
SHA1	43d80e5f8416185473dcaf83cb7f160d1eceefd2
SHA256	c7d23247432db58196e46661d9abe440a36d478fe9142da1ed73c37978e905c0
SSdeep	3072:rH+ywv9EfGdHLMHVZRVwO6PfMXoff6EWZ+xImimV3qraz4Wh1cwW/12WA5c+s6dB:7KHLMvdkfmBEWZ+amiamwVi+s6D
Imphash	84bf21e06080a07068692a185e3de384
Note	Alina POS Malware (HTTPS/SSL & DNS Variant)
C2 - DNS Request(s)	analytics-akadns[.]com testttdomain
C2 - HTTP Request(s)	hxxps://testttdomain/wp-admin/gate1.php
Sample	1.5

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 5:57 AM 4/11/2018
Certificate Common Name: GESO LTD
Certificate SHA-1 Thumbprint: 744160F36BA9B0B9277C6A71BF383F1898FD6D89
Certificate Serial Number: 00 B7 E0 CF 12 E4 AE 50 DD 64 3A 24 28 54 85 60 2F

Service Installation

The loader executes the dropped variant of Alina POS Malware using the "install" command line option. The "install" option will choose 1 of 30 different hard-coded service profiles and register the Alina POS malware as a service along with a persistence registry key and location.

Self-Deletion

After installation of the Alina POS Malware, the loader pauses briefly (ping wait) and then deletes itself with the following command:

```
cmd.exe /c ping localhost -n 3 > nul & del "<path_to_loader>" & exit
```

2. AlinaPOS - Section #2

The following malware samples share a **similar C2 domain** (akamai-analytics[.]com) as the **Alina POS Malware (DNS Variant)** used in the recent merchant breach.

Malware sample 2.1

Compile Time: 2019-03-16 17:08:36

Source	Virus Total
MD5	17777257e2bf877c5490619354b8116b
SHA1	6fdd747d03ac7d52fcb9f9e05c7d96214426ae4d
SHA256	da4f5802f333e96e2263080e8b8cf50db25aaab98d883f85724df63ce7111e12
SSdeep	3072:SQPM1QW/t/C0OSvUzB63kaK4ifBasaasq83KVq4grtnsk2m+:kGs/C0OSczSzCsRaqttsks
Imphash	98265794440757bc00036f7b67d88c98
Note	Alina POS Malware (DNS Variant)
C2 - DNS Request(s)	akamai-analytics[.]com
Sample	2.1

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 11:06 AM 3/16/2019
Certificate Common Name: P2N ONLINE LTD
Certificate SHA-1 Thumbprint: 2835F7084DF40A2D328AD3E251B9B95BBC8A1FD7
Certificate Serial Number: 61 DA 67 6C 1D CF CF 18 82 76 E2 C7 0D 68 08 2E

Malware sample 2.2

Compile Time: 2019-03-16 15:14:39

Source	Virus Total
MD5	dca7c29a79d21bfe9081e4c227bdad79
SHA1	7ad0c94e3eeab05b5add22d9b1cf614848b06a13
SHA256	30feb4ec6cab08452f5fa15e6c07df09777b90c4557f23e5be56eed433278800
SSdeep	3072:tQPM1QW/t/C0OSvUzB63kaK4ifBasaasq83KVq4grtnsk250:DGs/C0OSczSzCsRaqttskP
Imphash	98265794440757bc00036f7b67d88c98
Note	Alina POS Malware (DNS Variant)
C2 - DNS Request(s)	akamai-analytics[.]com
Sample	2.2

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 9:12 AM 3/16/2019
Certificate Common Name: P2N ONLINE LTD
Certificate SHA-1 Thumbprint: 2835F7084DF40A2D328AD3E251B9B95BBC8A1FD7
Certificate Serial Number: 61 DA 67 6C 1D CF CF 18 82 76 E2 C7 0D 68 08 2E

3. AlinaPOS - Section #3

The following malware samples **share some similarities**, such as structural code similarities, shared signing certificate, and C2 domain infrastructure, as the **Alina POS Malware (DNS Variant)** used in the recent merchant breach.

Malware sample 3.1

Compile Time: 2018-11-26 02:44:09

Source	Virus Total
MD5	c84b393b2628ecd4df1b4f10913c6370
SHA1	1e3d0d2f7bc06aeda6a61a13e33013e025daa1aa
SHA256	6c6166c356ee2f92b32ad597edcdb34309ba4e7b281801b85fab95a6543a97db
SSdeep	3072:u73QHwn7YMzN5bkFxuy3U7qzxyeeiY5ddfkiuy41wRUnHB1r5NVyezVd:m7f3kFwzqz8e/YHPu5HzrfVyA
Imphash	06f6f9f730bc6497744fe801a88b435e
Note:	Alina POS Malware (DNS Variant)
C2 - DNS Request(s)	akamai-information[.]com
Note	3.1

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 8:42 PM 11/25/2018
Certificate Common Name: LSG IT Services Ltd
Certificate SHA-1 Thumbprint: 869ABB3E7C7086C913845B2D1B56EB8690549EF0
Certificate Serial Number: 24 AA 38 D6 A5 F8 8B 7F EC E7 57 71 05 69 1B 41

Malware sample 3.2

Compile Time: 2018-11-18 18:42:39

Source	Virus Total
MD5	cfba66f4ccdb5a0502ba90411c29803d
SHA1	ada32f0903829e64ebd2dd57da5c5f34cb83183d
SHA256	fd0e0f20ba1408080d0ff055aaac416a4ac53e958c0d2ec53de076787c125272
SSdeep	3072:73QPerK9RDtD5XZUlfZhW7BnfsUpJ6I9Ms9Go/1wWJqHSDBlIZN2ymh7:9KDB5XCrhW7FffJLE4jI/2y47
Imphash	06f6f9f730bc6497744fe801a88b435e
Note	Alina POS Malware (DNS Variant)
C2 - DNS Request(s)	akamai-technologies[.]com
Sample	3.2

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 12:40 PM 11/18/2018
Certificate Common Name: CIF Consulting Limited

Certificate SHA-1 Thumbprint: BBAD97799B36BBBEBF2B3FD01943F8135B567E4C
Certificate Serial Number: 18 C1 EA 75 99 C8 C6 1E 6C 79 05 F6 44 50 B6 B0

Malware sample 3.3

Compile Time: 2018-02-07 21:25:02

Source	Virus Total
MD5	dd6e1bc77e1b0ad291126ed4175ba48d
SHA1	968b8b8926ec1514dc053d8a29b41bcabada6825
SHA256	c01a7be3a05a1971acffea1e8399f18ed627277321236a497700bbf32c08ec3c
SSdeep	3072:8YRZOh+ehcF+tXOK/7I3lXPzOf6as9l3SuUQRQLLMmEbv1rlpq8hwkeZF0yTXj:DUFOK/k3lLOf6akCufoew86dn0yX
Imphash	2935c338b75c9786a45b63151e8e4172
Note:	Alina POS Malware (HTTPS/SSL Variant)
DNS Request(s)	profile.sandoct[.]com
HTTP Request(s)	hxxp://profile.sandoct[.]com/wp-200/gate1.php
Sample	3.3

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 12:40 PM 11/18/2018
Certificate Common Name: CIF Consulting Limited
Certificate SHA-1 Thumbprint: BBAD97799B36BBBEBF2B3FD01943F8135B567E4C
Certificate Serial Number: 18 C1 EA 75 99 C8 C6 1E 6C 79 05 F6 44 50 B6 B0

Malware sample 3.4

Compile Time: 2017-12-21 04:02:25

Source	Virus Total
MD5	07420893a9136686d9040b9c3fe7249d
SHA1	edf27025d326ea84fae1ef3925823d7a91f5b9d6
SHA256	23668f38b9a10859302070a606cabd313e1b84ed5be81bd26c2d9bda29ebffa9
SSdeep	3072:rzRZOh+ehcF+tXOK/7I3lXPzOf6as9l3SuUQRQLLMmEbv1rlpq2VwkrZF0ymX7:jUFOK/k3lLOf6akCufoew220n0yO
Imphash	2935c338b75c9786a45b63151e8e4172
Note:	Alina POS Malware (HTTPS/SSL Variant)
DNS Request(s)	www[.]ambertut[.]com
HTTP Request(s)	hxxp://www[.]ambertut[.]com/wp-206/gate1.php
Sample	3.4

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 10:01 PM 12/20/2017
Certificate Common Name: GESO LTD

Certificate SHA-1 Thumbprint: 744160F36BA9B0B9277C6A71BF383F1898FD6D89
Certificate Serial Number: 00 B7 E0 CF 12 E4 AE 50 DD 64 3A 24 28 54 85 60 2F

4. Deployment Loader

PFD assesses that the Alina POS (DNS variant) samples, as identified in the recent merchant breach, were deployed into the target environment using a deployment loader. The deployment loader functions as follows:

- **Deployment** - the loader deploys a variant of Alina POS malware into a POS specific folder.
- **Execution** - the loader executes the dropped variant of Alina POS using the "install" command line option. The "install" option will choose 1 of 30 different hard-coded service profiles and register the malware-as-a-service along with a persistence registry key and location.
- **Self-Deletion** - After installation of the malware, the loader pauses briefly (ping wait) and then deletes itself.

File Name	bcastdvs.exe / OneDriveUi.exe
Source	Virus Total
MD5	d000bd7c56811eec4067a4b7401bcb38
SHA1	f5e89c72f62ea9a51161b2e1407c719903308e41
SHA256	c55b2f3b67108a58c4cb81c3550115956cb07139e39a37ce9eb57ff4fb41d832
SSdeep	3072:VV3QHwn7YMzN5bkFxuy3U7qzxyeeiY5ddfkiuy41wROrHB1O5NVyT8:D7f3kFwzqz8e/YHPuLTzOfVyg
Note	Alina POS Malware (DNS Variant)
Sample	4
DNS Request(s)	zuzn4v_EkO7l5OX86-SH-umQm5DjxNney8bG.analytics-akadns[.]com yczA8vzDkO7l5OX86-SH-umQm5D53svY3g.analytics-akadns[.]com yczA8vzDkO7l5OX86-SH-umQm5D6w8TN.analytics-akadns[.]com yczA8vzDkO7l5OX86-SH-umQm5CQ2sXZhM_Sz5CQmZycmZ2dkpmTkpOemJ2cl5.iYm5uYmpuampqampqbk5mam5qampqampKdnZqamg.analytics-akadns[.]com

Authenticode Signature Block
Signature verification: Signed file, valid signature
Signing Date: 10:23 AM 1/10/2019
Certificate Common Name: FIRNEEZ EUROPE LIMITED
Certificate SHA-1 Thumbprint: 91BCEBBFC1C3EB8F60D958FCFE20E648F6ED6507
Certificate Serial Number: 00 B1 DA 21 96 88 E5 1F D0 BF AC 2C 89 1D 56 CB B8

Process Blacklist

During execution, the Alina POS malware scans running processes and blacklists applications that would typically not contain credit card track data. This specific variant of Alina POS contains **76 different processes** in its process blacklist.

Credit Card Data Log

This variant creates a file named "**wshelper.cache.dll**" in the current directory where it logs scraped payment account data in plain text.

Encrypted Backup Copy

During execution, the Alina POS Malware creates a RC4 encrypted backup copy of itself (**RC4 Key** = 12345678) in the following location: %APPDATA%**4687453546776.tmp**

Recommendations for Issuers and Acquirers

1. Visa recommends Issuers and Acquirers take the following actions to mitigate against these threats:
    - **Check local area networks** for IOC's included in this report.
    - **Secure remote access** with strong passwords, ensure only the necessary individuals have permission for remote access, and disable remote access when not in use.
    - **Enable EMV technologies** for secure in-person payments (chip, contactless, mobile and QR code).
    - **Provide each Admin user with their own user credentials**. User accounts should also only be provided with the permissions vital to job responsibilities.
    - **Turn on heuristics (behavioral analysis) on anti-malware** to search for suspicious behavior, and update anti-malware applications.
    - **Monitor network traffic** for suspicious connections, and log system and network events.
    - **Implement Network Segmentation**, where possible, to prevent the spread of malicious software and limit an attacker's foothold.
    - **Maintain a patch management program** and update all software and hardware firmware to most current release to limit the attack surface for zero-day vulnerabilities.
    - **Refer to Visa's *What to Do If Compromised (WTDIC)* document**, published August 2016:

2. Refer to the following resources for more information on security standards, PCI compliance requirements, and best practices:
    - PCI Data Security Standard Quick Reference Guide
    - Refer to Visa's Card Acceptance Guidelines for Visa Merchants
    - Additional information on PCI DSS can be found at www.pcissc.org

Contact Information

For more information, please contact paymentintelligence@visa.com

Disclaimer:
This report is intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa is not responsible for your use of the information contained in this report (including errors, omissions, or non-timeliness of any kind) or any assumptions or conclusions you may draw from it. All Visa Payment Fraud Disruption Situational Intelligence Assessment content is provided for the intended recipient only, and on a need-to-know basis. PFD reporting and intelligence are intended solely for the internal use of the individual and organization to which they are addressed. Dissemination or redistribution of PFD products without express permission is strictly prohibited.