# Alina Point of Sale Malware Still Lurking in DNS

blog.centurylink.com/alina-point-of-sale-malware-still-lurking-in-dns/

July 1, 2020

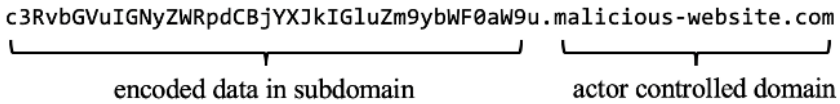
Black Lotus Labs Posted On July 1, 2020



As we've previously written, adversaries continue to ramp up DNS-based attacks to support a wide range of criminal activities. As part of our mission to leverage our network visibility to both help protect customers and keep the internet clean, Black Lotus Labs monitors global DNS traffic for anomalous behavior that may be malicious. One of our machine learning models recently flagged unusual queries to the domain akamai-technologies[.]com1, and

upon decoding the information contained in the subdomains of these queries, uncovered what was revealed to be credit card information being exfiltrated by the Alina Point of Sale (POS) malware.

Credit card processing systems typically run in Windows environments, allowing them to be targeted by the existing skills of the crimeware markets. Due to the strict security restrictions applied to credit card processing, HTTP and other common outbound traffic may be highly restricted in these environments. However, DNS is often left available, and too commonly goes unmonitored. This makes DNS an attractive choice for outbound communication in POS malware, including the exfiltrating of stolen credit card information. Malware authors encode the stolen information and issue a DNS query to the actor-controlled domain name. The encoded data is placed in a subdomain, which the malicious actors then extract when they receive the DNS query.




The malicious actors then sell this information in underground criminal markets. The number of credit card numbers for sale in underground forums tripled in the second half of 2019 compared to the first six months of the year, making POS malware an opportunity to participate in an unfortunately thriving criminal market2.

## Alina Malware Deep Dive

After identifying the akamai-technologies[.]com domain, we found three other domains with similar DNS queries. Further research showed these domains as being used by the Alina POS malware3.

analytics-akadns[.]com

akamai-analytics[.]com

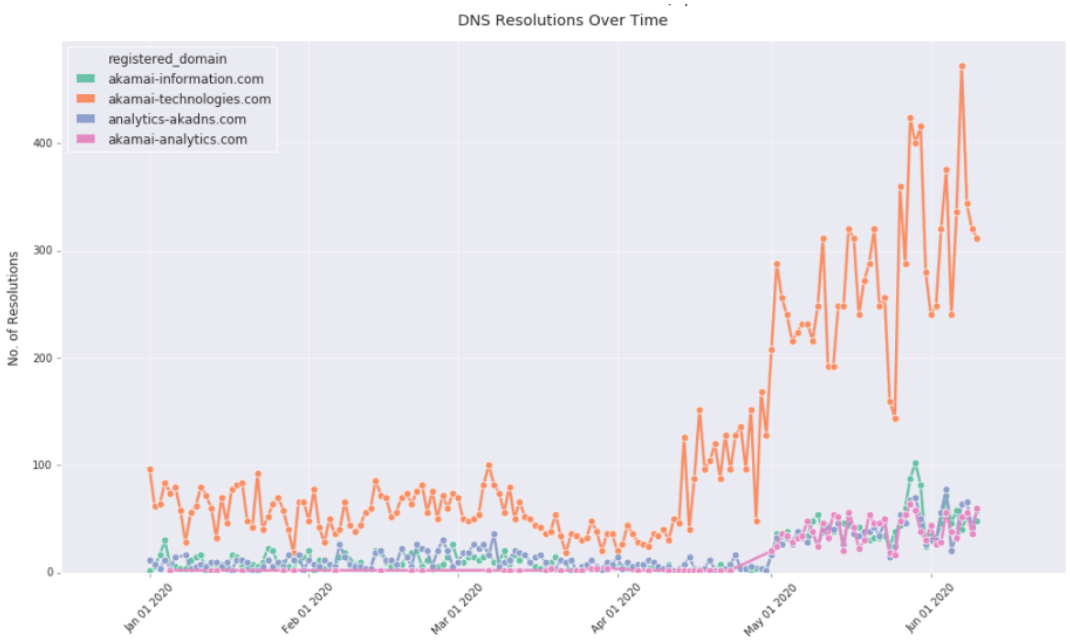
akamai-information[.]com

akamai-technologies[.]com

The POS devices that complete credit card transactions can vary greatly. They may be separate hardware devices, but in smaller retail environments it may be a regular desktop computer running the POS software. During the credit card transaction, the data is typically decrypted and is temporarily in the POS software's memory in unencrypted form. The malware searches the RAM of the POS device for this unencrypted credit card information and sends it back to a Command and Control (C2) server. To ensure that only real credit card data is found when searching the RAM of the device, the malware verifies that the last digit of the card number is the correct check digit4 using the Luhn checksum algorithm5.

Since it was first discovered in 2012, the malware authors behind Alina have evolved their Tactics, Techniques and Procedures (TTPs) to evade detection. While earlier samples of the malware used HTTPS or a combination of HTTPS and DNS for the exfiltration of the stolen credit card information, samples seen starting in late 2018 use DNS exclusively for communication3.

Below are the volume of queries Black Lotus Labs observed to each of the C2 domains since January 2020. We can see that after a decrease in traffic in April, there has been an increase in traffic to all the domains, especially akamai-technologies[.]com, since the beginning of May. This increase in traffic is due to queries originating from a single victim from the financial services industry.




DNS queries to the C2 domains are all type A queries, meaning they are expecting an ipv4 response. They all have random-looking subdomains, such as the following query:

yeTLxcbvkOjr6eH_-pCYkPrDxM0.akamai-technologies[.]com

Black Lotus Labs was able to decode the encoded subdomains. First, characters that are not allowed in DNS queries according to the DNS protocol specification must be replaced by their original characters:

“-” is replaced with “/”

“_” is replaced with “+”

Then the resulting subdomain can be base64 decoded, by adding trailing “=” characters if necessary. Finally, this decoded data is XORed with the byte 0xAA. This XOR value was used in previous versions of the malware that utilized HTTP POST messages for

communication[6]. Using this algorithm, we can see the exfiltrated data from the decoded subdomains.

cNaolE:BACKTT:2:Ping

YaKNsY:BACKOFFICEz2::ddcdsrv1.exe::<Credit card digits removed>

The first six characters of the decoded queries appear to be an ID value consisting of upper- and lower-case letters that is unique to each victim. Every communication from the victim starts with this unique ID. This is similar to the random characters chosen by the malware as a unique identifier in previous versions[6].

The character ":" is used as a delimiter in the decoded data. Following the ID field is a descriptor or location field, such as "BACKTT" or "BACKOFFICEz2" in the above data. We have also observed values such as "TERMINAL1." It is unclear what this represents, but given the names observed this may be the system name of the computers infected with the malware.

Each of the DNS queries uncovered are either checking in with the C2, such as the "Ping" query above, or they contain credit card information. The queries that contain credit card numbers contain an executable name in the field following the location or descriptor field. This appears to be the process which the malware identified as containing the credit card information in memory. Earlier samples of the malware either contained a list of processes to examine, or examined every process running except for those contained in a list of processes to ignore[7].

Some of the processes found in the decoded data, which are shown below, were seen in the list of processes to examine in previous versions of the malware[7].

CreditCardService.exe

DSIMercuryIP_Dial.exe

EdcSvr.exe

fpos.exe

Below are other processes we observed in the decoded data. Some of these, such as "ddcdsrv1.exe," have been targeted by other POS malware[8].

Brain.exe

Focus.exe

appidt.exe

ddcdsrv1.exe

fontdvrhost.exe

tcopy.exe

The final field in the decoded data begins with the credit card number, followed by “=” and the expiration date, in the following format. The final seven digits are unclear.

<Credit card digits removed>=DDMMYYYY<Unknown seven digits>

For most of the queries, the response given in DNS by the actor’s authoritative name server is 127.0.0.1. Examining the IPs hosting the name servers for the C2 domains, we came across another suspicious domain, sync-akamai[.]com. The name server for this domain was hosted on the same IP as ns1.akamai-analytics[.]com. While we have not seen any data exfiltration to this domain yet, it should be monitored as well.

DNS is a popular choice for malware authors to bypass security controls and exfiltrate data from protected networks. Point of Sale malware continues to pose a serious security threat, and malicious actors regularly update their malware in efforts to evade detection. At Black Lotus Labs, we use machine learning algorithms to identify data exfiltration and other anomalous DNS traffic. We have reached out to our customers impacted by the Alina malware and the registrars of the malicious domains, and will continue to monitor the malicious domains as we work to eliminate the exfiltration of data in the CenturyLink global DNS traffic. We recommend all organizations, including retailers using point of sale systems, to monitor DNS traffic for suspicious queries.

## IoCs

analytics-akadns[.]com

akamai-analytics[.]com

akamai-information[.]com

akamai-technologies[.]com

sync-akamai[.]com

140.82.60[.]233

104.238.133[.]172

144.202.59[.]50

66.42.118[.]249

198.54.117[.]197

198.54.117[.]198

198.54.117[.]199

198.54.117[.]200

fd0e0f20ba1408080d0ff055aaac416a4ac53e958c0d2ec53de076787c125272

c01a7be3a05a1971acffea1e8399f18ed627277321236a497700bbf32c08ec3c

fd0e0f20ba1408080d0ff055aaac416a4ac53e958c0d2ec53de076787c125272

c01a7be3a05a1971acffea1e8399f18ed627277321236a497700bbf32c08ec3c

23668f38b9a10859302070a606cabd313e1b84ed5be81bd26c2d9bda29ebffa9

c55b2f3b67108a58c4cb81c3550115956cb07139e39a37ce9eb57ff4fb41d832

804559ea57381bd6c2301d0c9393cf3768e54455ece74acdb99bb307f80494eb

83e3df5ec961ce9b24588ba95025ce94e34c319a8afa30fab2b7cca10c0ef904

c7d23247432db58196e46661d9abe440a36d478fe9142da1ed73c37978e905c0

da4f5802f333e96e2263080e8b8cf50db25aaab98d883f85724df63ce7111e12

30feb4ec6cab08452f5fa15e6c07df09777b90c4557f23e5be56eed433278800

6c6166c356ee2f92b32ad597edcdb34309ba4e7b281801b85fab95a6543a97db

c0b4ab7a897102ceea5ce82a36018cb5d20806dd47db61484c4ea8e331a423c7

0ae4740e74f7350adb13b23e5a2094b2821aafb49ec122a789b1e98ee93458fd

This information is provided “as is” without any warranty or condition of any kind, either express or implied. Use of this information is at the end user’s own risk.

1 The domains that experienced the suspicious DNS traffic were neither owned nor managed by Akamai. As of the date of this publication, Akamai was actively collaborating with Black Lotus Labs to take down the imposter domains.

2 https://blog.cybersixgill.com/dark-web-financial-fraud-2019

3 https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-alina-pos-malware.pdf

4 https://twitter.com/VK_Intel/status/1123463742958768128

5 https://en.wikipedia.org/wiki/Luhn_algorithm

6 https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/alina-pos-malware-sparks-off-a-new-variant/

7 https://www.pandasecurity.com/mediacenter/pandalabs/alina-pos-malware/

8 https://www.proofpoint.com/us/threat-insight/post/ostap-bender-400-ways-make-population-part-with-their-money

---

Black Lotus LabsCybersecurityCybersecurity AttacksMalware


Author

**Black Lotus Labs**

The mission of Black Lotus Labs is to leverage our network visibility to help protect customers and keep the internet clean.