MULTIGRAIN – Point of Sale Attackers Make an Unhealthy Addition to the Pantry

fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html

FireEye recently discovered a new variant of a point of sale (POS) malware family known as NewPosThings. This variant, which we call “MULTIGRAIN”, consists largely of a subset of slightly modified code from NewPosThings. The variant is highly targeted, digitally signed, and exfiltrates stolen payment card data over DNS. The addition of DNS-based exfiltration is new for this malware family; however, other POS malware families such as BernhardPOS and FrameworkPOS have used this technique in the past.

Using DNS for data exfiltration provides several advantages to the attacker. Sensitive environments that process card data will often monitor, restrict, or entirely block the HTTP or FTP traffic often used for exfiltration in other environments. While these common internet protocols may be disabled within a restrictive card processing environment, DNS is still necessary to resolve hostnames within the corporate environment and is unlikely to be blocked.

Specific Targeting

Several POS malware families will parse through running processes and scrape a large number of them in the hopes of locating card data. In contrast to that approach, MULTIGRAIN has been custom-engineered to target a specific point of sale process:

multi.exe, associated with a popular back-end card authorization and POS (electronic draft capture) server software package. If *multi.exe* is not found on the infected host, the malware will not install and will simply delete itself. This shows that while developing or building their malware, the attackers had a very specific knowledge of the target environment and knew this process would be running.

Persistence

If the targeted POS process is running on the host and the malware is executed with a command line parameter designating "installation mode", MULTIGRAIN copies itself to the hardcoded location "*c:\windows\wme.exe*" and installs a service with the properties shown in Figure 1.

```
display name: Windows Module Extension
service name: Windows Module Extension
service type: SERVICE_WIN32_OWN_PROCESS
start type  : SERVICE_AUTO_START
path        : C:/Windows/wme.exe
```

Figure 1: Service properties used by MULTIGRAIN POS malware

Initial Beaconing

The malware collects the volume serial number and part of the MAC address and creates a hash of the concatenated value using the DJB2 hashing algorithm. The resulting hash is then combined with the computer name and a version number and all three components are then encoded with a custom Base32 encoding algorithm. The malware then makes a DNS query with this information to a hardcoded domain, notifying the attacker of a successful installation. The process is shown in Figure 2.

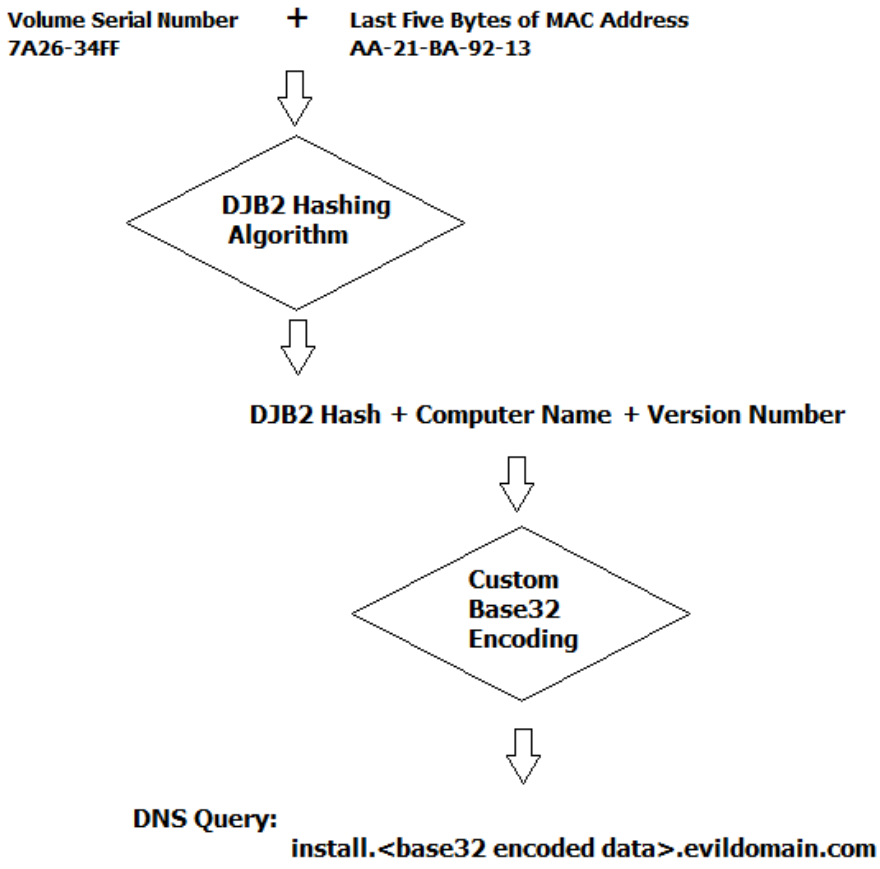


Figure 2. Construction of Installation Beacon

Memory-Scraping and Card Data Exfiltration

Once installed and executing, MULTIGRAIN begins scraping the memory of the targeted process for Track 2 card data, validating that data using the Luhn algorithm. Track 2 data will normally contain the PAN (Primary Account Number), Expiration Date, Service Code and optionally a CVV/CVC number, data which will typically be sufficient in most scenarios to attempt "card-present" and, and in some cases, "*card-not-present*" fraud.

Each Track 2 record is first encrypted with a 1024-bit RSA public key, pushed through the same custom Base32 encoding process as used in the installation beacon, and then stored in a buffer. Every five minutes, the malware checks this buffer to see if any card data is ready for exfiltration. If card data is present, the individual encrypted and encoded Track 2 data record for each card is sent over the network by means of a DNS query made by the malware. The process is shown in Figure 3.

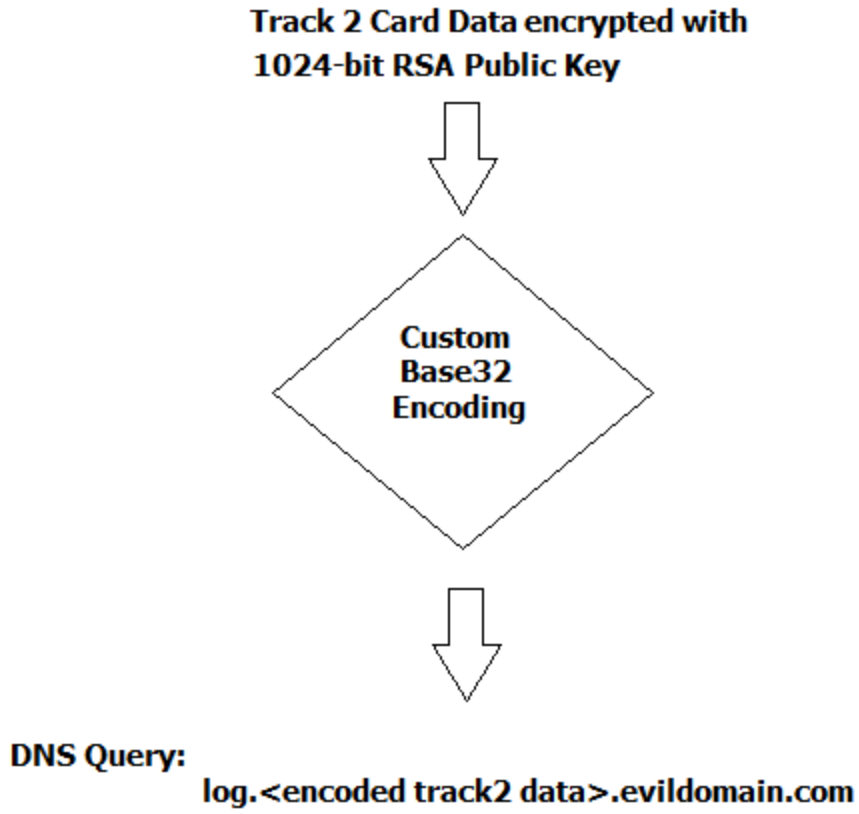


Figure 3. Track 2 Card Data Encoding and Exfiltration

Base32 Encoding

Both the installation beacon and the stolen card data are encoded with an unusual encoding algorithm – Base32 – before being transmitted via DNS queries. The choice of Base32 is interesting as Base64 is better known and more widely used (for instance in the MIME standard used by email attachments). Using Base32 will actually result in the data taking up 20 percent more space than Base64, so the attackers were unconcerned with the efficiency of bandwidth.

One possible reason for selecting Base32 is the relative obscurity of the algorithm. Security and data loss prevention (DLP) products are more likely to detect Base64 encoding and in some cases can automatically decode the data, which could result in DLP devices identifying the exfiltration.

Code Reuse

Elements of the code from MULTIGRAIN show strong similarities to the POS malware family known as NewPosThings. Shared code elements include:

- The code used to scrape a process for card data
- The DJB2 hashing algorithm used as part of creating a system ID

Two other examples from binary disassembly are shown below: the "*connect/3*" network beacon (Figure 4 – seemingly unused in MULTIGRAIN) and similarities in the construction of the installation beacon (Figure 5).

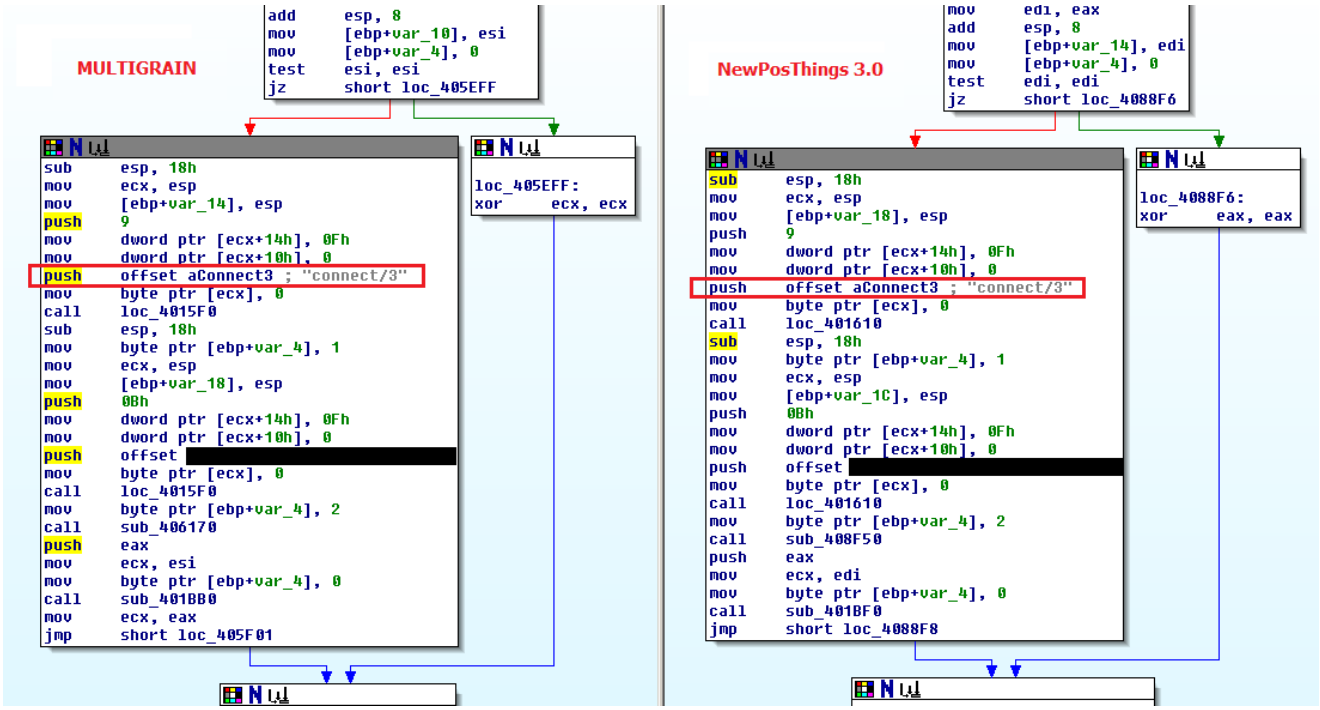


Figure 4. "Connect/3" network beacon comparison between MULTIGRAIN and NewPosThings

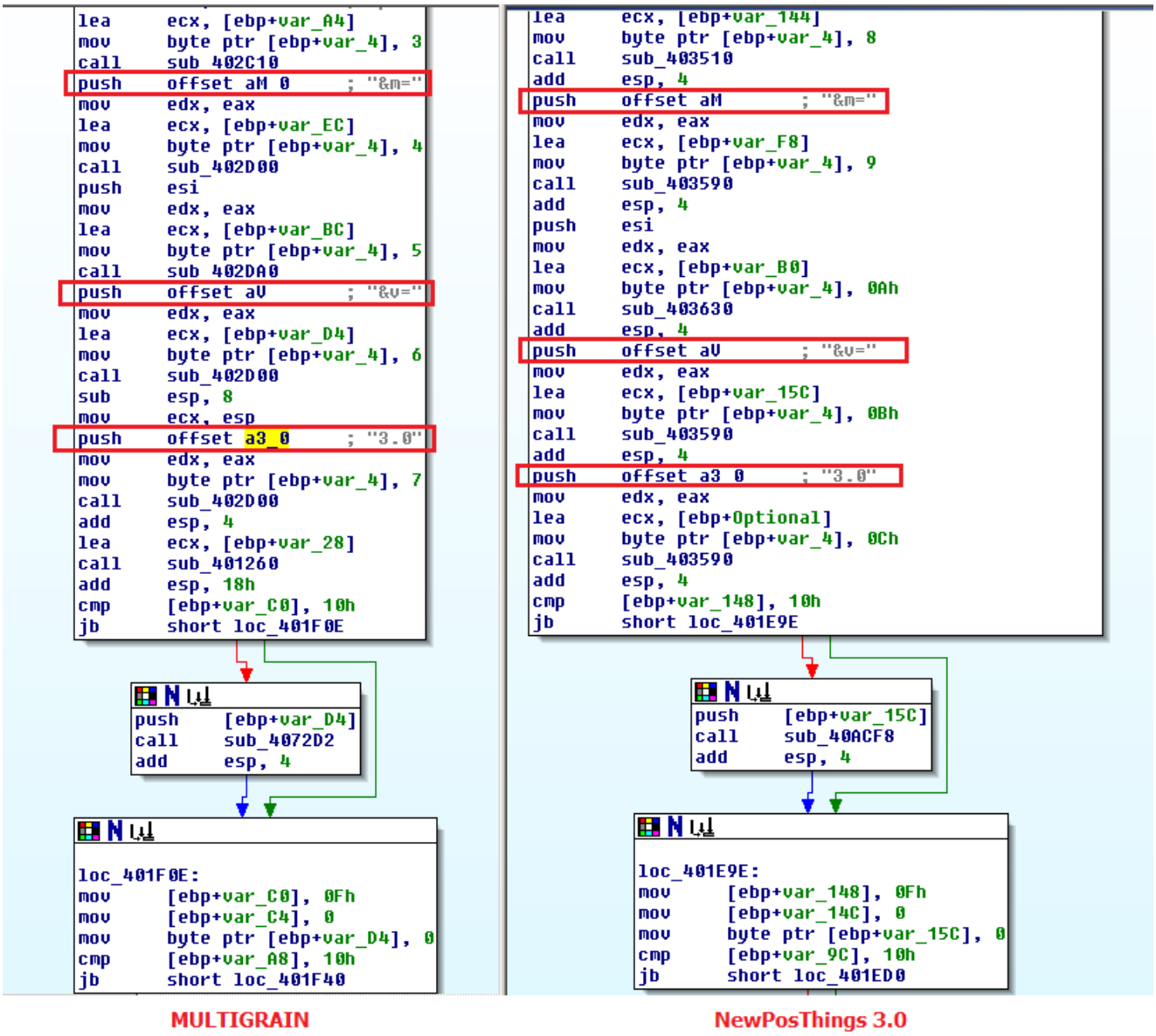
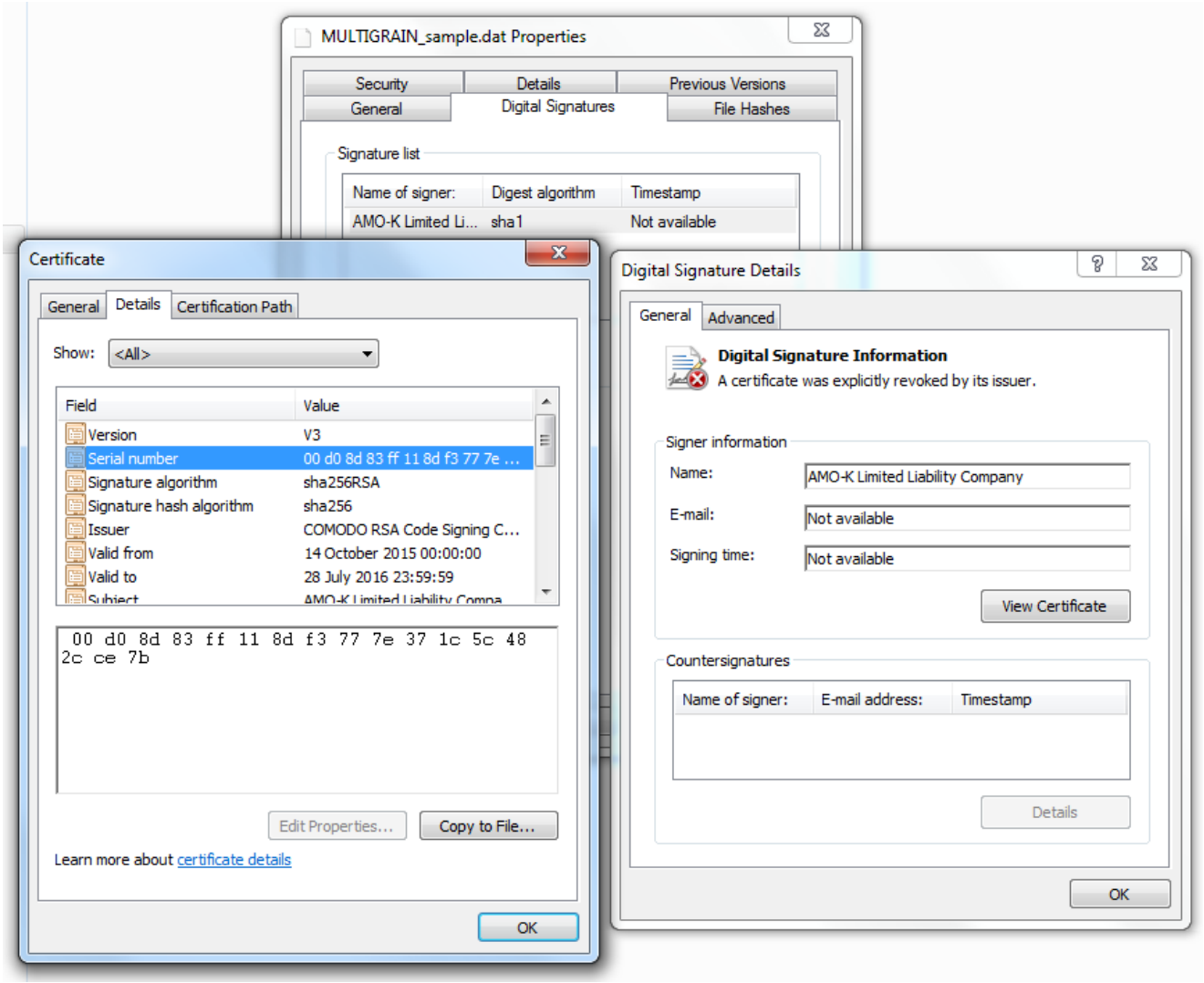


Figure 5. Installation beacon comparison between MULTIGRAIN and NewPostThings

Digital Signature

As shown in Figure 6, this MULTIGRAIN sample is digitally signed with a certificate issued to the “AMO-K Limited Liability Company” with a *Comodo* root and intermediate certificate chain (serial number d0 8d 83 ff 11 8d f3 77 7e 37 1c 5c 48 2c ce 7b). The certificate was revoked on Oct. 14, 2015.


MULTIGRAIN_sample.dat Properties
Security
Details
Previous Versions
General
Digital Signatures
File Hashes
Signature list
Name of signer:
Digest algorithm
Timestamp
AMO-K Limited Li...
sha1
Not available
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
00 d0 8d 83 ff 11 8d f3 77 7e ...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
COMODO RSA Code Signing C...
Valid from
14 October 2015 00:00:00
Valid to
28 July 2016 23:59:59
Subject
AMO-K Limited Liability Compa
00 d0 8d 83 ff 11 8d f3 77 7e 37 1c 5c 48
2c ce 7b
Edit Properties...
Copy to File...
Learn more about certificate details
OK
Digital Signature Details
General
Advanced
Digital Signature Information
A certificate was explicitly revoked by its issuer.
Signer information
Name:
AMO-K Limited Liability Company
E-mail:
Not available
Signing time:
Not available
View Certificate
Countersignatures
Name of signer:
E-mail address:
Timestamp
Details
OK

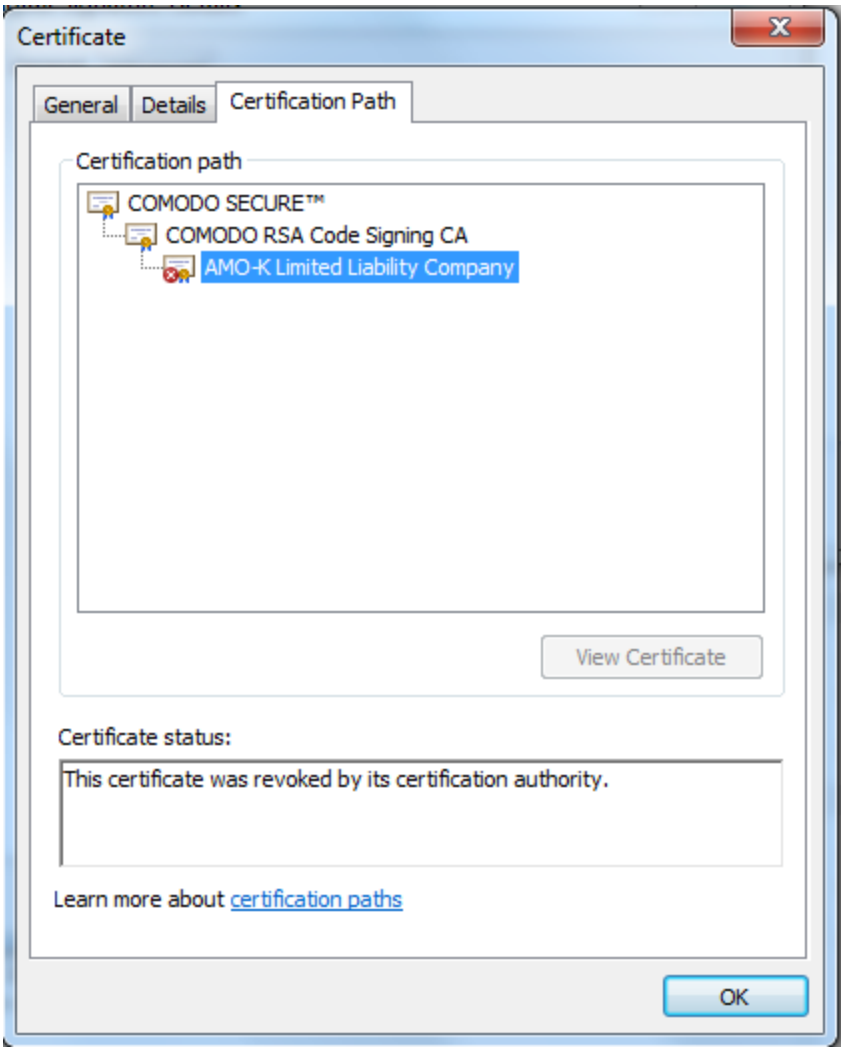


Figure 6: Digital certificate used to sign MULTIGRAIN sample

Conclusion

Organizations that process card data must remain vigilant against attackers intent on financial fraud. Many POS malware families are written to be fairly generic (for example, targeting any process that may contain payment card data). However, threat actors may operate with greater stealth, customizing malware for specific environments and using less common protocols or methods for data exfiltration.

Although MULTIGRAIN does not bring any new capabilities to the POS malware table, it does show that capable attackers can customize malware “on-the-fly” to target a specific environment. While exfiltration via DNS is not a new tactic, MULTIGRAIN demonstrates that organizations should monitor and review DNS traffic for suspicious or anomalous behavior.

MD5:

F924CEC68BE776E41726EE765F469D50

This post was first available on Visa Threat Intelligence, the first product available from the partnership between Visa Inc. and FireEye. Subscribers will gain access to a powerful web portal that distills the latest proprietary cyber intelligence relevant to payment systems into actionable information, including timely alerts on malicious actors, methods, trends in cyber-attacks, and in-depth forensic analysis from recent data beaches. Contact your Visa Account Executive or email VisaThreatIntelligence@Visa.com for more information.