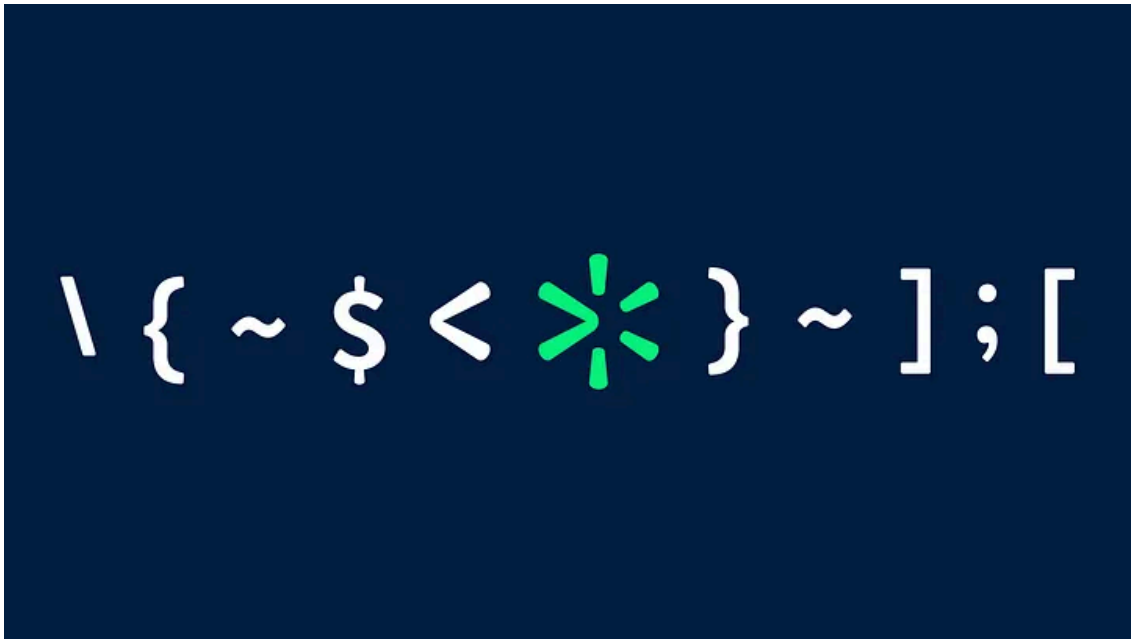
Anchor and Lazarus together again?

By Jason Reaves

Published: 2021-01-20 · Archived: 2026-04-05 16:07:38 UTC

Press enter or click to view image in full size



On 6 July 2020 SanSec reported that North Korea APT group dubbed Lazarus/HIDDEN COBRA, was performing MageCart style attacks against websites[1].

Two mentions in their report are interesting, PaperSource and FocusCamera[1].

Press enter or click to view image in full size

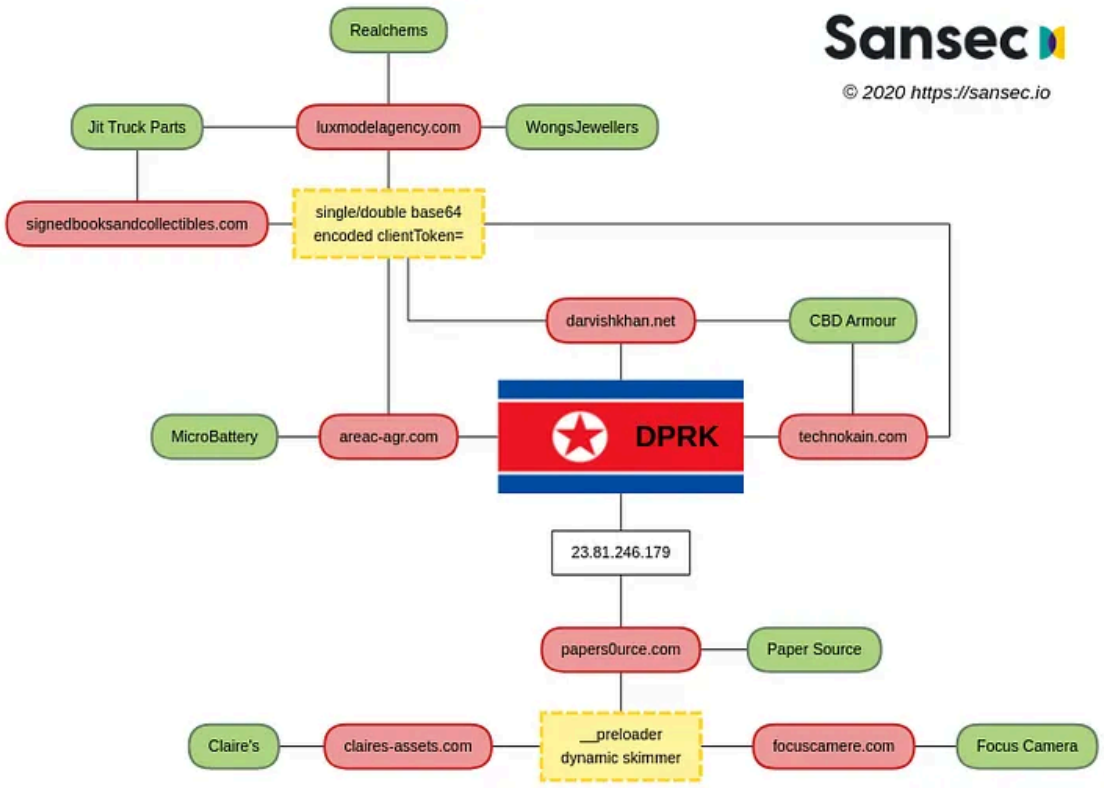


Photo Credit: SanSec

The entire North Korea link appears to hinge on a IP reuse for an IP in LeaseWeb which is a weak link for attribution but sometimes there could be non public details about the incident. The more interesting aspect to this is some context that we can provide to the story, namely the connection to TrickBot/Anchor. You may recall that this would not be the first time this CyberCrime crew has been caught working with Lazarus.

Also interesting from the article “The malware was removed within 24 hours but a week later, the very same malware resurfaced on the same store.”[1] which would suggest the attackers had a foothold or “Anchor” into the environment.

FocusCamera

This name immediately stood out after reading the SanSec report, it came up during our previous work revolving around PowerTrick[4] which is the powershell framework developed and utilized by TrickBot/Anchor actors. The company appears to of been initially breached by TrickBot around October 2019 and actors then began using PowerTrick to pivot around.

```
3|C:\WINDOWS\system32|NYIT581|FC\NYIT581$|NT AUTHORITY\SYSTEM|4C4C4544-004C-4310-8031-CAC04F575231|M
```

PowerTrick bot listing network devices:

```
\\101718-1628
\\101718-1900
\\11012018-1018
```

```
\\111218-1913
\\ABE-NEW
\\CONNCESHIPSRV
\\CONNECTSHIP
\\DES-0001
\\FBARETURN
\\FCNYAV1              fcnyav1
\\FCNYMAIL1
\\FOCUSCA-782GU8N
\\FOCUSCA-9146562
\\FOCUSCA-MGL6SO0
\\FOCUSCA-QHRB0KS
\\FOCUSCA-UIHGRK3
\\LKWD-20
\\MICHAELBACK
\\MONSOONSERVER
\\NAS-BF-27-4E         nas-BF-27-4E
\\NASBACKUP            nasbackup
\\NEW01
\\NY-061418-1757
\\NY-062918-1421
\\NY-100318-1432
\\NY-AMZ-002
\\NY-AMZN-060618       Hudy kryman
\\NY-BUY-003
\\NY-BUYER-AA          yoni Baum
\\NY-CONF-01
\\NY-CONF-02
\\NY-CONF-03
\\NY-ER-CCTV-SCRN
\\NY-KIT-070318        miriam mozyrskiy
\\NY-KIT-BILECKI
\\NY-LGSTC-PHILIP
\\NY-MARKETING         Isaac Shalev
\\NY-MINCHA
\\NY-REFURB-0001
\\NYACCT-0001
\\NYACCT162
\\NYACT004
\\NYACT179
\\NYACT180
\\NYACT183
\\NYACT188
\\NYACT189
\\NYASS178A
\\NYASST159
\\NYASST193
```

```
\\NYBUY0001            Robert Silberman - Buyer
\\NYBUY078
\\NYBUY102
\\NYBUY148
\\NYBUY149
\\NYBUY151
\\NYBUY151A
\\NYBUY153
\\NYBUY165
\\NYBUY209
\\NYBUY210
\\NYBUY303
\\NYBUY306
\\NYBUY307
\\NYBUY331
\\NYBUY333
\\NYBUY343
\\NYBYD151A
\\NYCAMERA01
\\NYCUSV049A
\\NYCUSV065
\\NYCUSV071
\\NYCUSV084
\\NYDC
\\NYDOMAINCTRL
\\NYEBAY002
\\NYEBAY128
\\NYEBAY345
\\NYFBA349
\\NYFBA351
\\NYGOV101
\\NYHR007
\\NYIT054              Chaim Geller
\\NYIT087
\\NYIT097
\\NYIT335
\\NYIT350
\\NYIT353
\\NYIT355
\\NYIT355A
\\NYIT581
\\NYKEYACCESS          NYKEYACCESS.FC.LOCAL
\\NYKIT-001
\\NYMAN164A
\\NYMGMT-RBERG
\\NYMGMT243BBB
\\NYOVER007
```

```
\\NYRCV001
\\NYRTNS141
\\NYRTNS281
\\NYRTNS285
\\NYSALES349
\\NYVIRTUALPC05
\\NYWAL347
\\NYWARE282A
\\NYWEB0001            car byers
\\REFURDBASE
\\SCRAPER-PC
\\STORE-01             Cashier-01
\\STORE-02             Cashier-02
\\STR-CCTV
\\VIEWPOINT
\\VMWAREVC
\\WHSE1
\\WINDOWS-0SD9E3K
\\WINDOWS-16M2FRN
\\WINDOWS-1O2SBEG
\\WINDOWS-851OD2Q
\\WINDOWS-HSDST7A
\\WINDOWS-I2SBFRI
\\WINDOWS-JNI13EQ
\\WINDOWS-Q88PP4L
\\WINDOWS-SQFPH6T
The command completed successfully.
```

PaperSource

We have reason to believe that PaperSource was also initially TrickBot and later Anchor and MemScraper which is their POS component of the Anchor Framework previously detailed[5].

Press enter or click to view image in full size

PaperSource MemScraper infection

Given these revelations we have two possibilities:

Get Jason Reaves's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

— The SanSec NK attribution is incorrect and TrickBot actors are also interested in leveraging jsSniffers against victim websites in MageCart style attacks.

— The SanSec NK attribution is correct and this is one more example of Lazarus being involved in TrickBot infected institutions.

By: Jason Reaves and Joshua Platt

References

1. https://www.zdnet.com/article/trickbot-gang-is-now-a-malware-supplier-for-north-korean-hackers/
2. https://sansec.io/research/north-korea-magecart
3. https://intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals/
4. https://www.darkreading.com/vulnerabilities---threats/trickbot-group-adds-new-powershell-based-backdoor-to-arsenal/d/d-id/1336769
5. https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/
