North Korean hackers are skimming US and European shoppers

6th July 2020 / Web Skimming / Sansec Threat Research Team

North Korean state sponsored hackers are implicated in the interception of online payments from American and European shoppers, Sansec research shows. Hackers associated with the APT Lazarus/HIDDEN COBRA[1] group were found to be breaking into online stores of large US retailers and planting payment skimmers as early as May 2019.

Previously, North Korean hacking activity was mostly restricted to banks and South Korean crypto markets[2], covert cyber operations that earned hackers $2 billion, according to a 2019 United Nations report[3]. As Sansec's new research shows, they have now extended their portfolio with the profitable crime of digital skimming.

Sansec researchers have attributed the activity to HIDDEN COBRA because infrastructure from previous operations was reused. Furthermore, distinctive patterns in the malware code were identified that linked multiple hacks to the same actor.

Digital skimming, also known as Magecart[4], is the interception of credit cards during online store purchases. This type of fraud has been growing since 2015 and was traditionally dominated by Russian-[5] and Indonesian-speaking[6] hacker groups. This is no longer the case, as the incumbent criminals now face competition from their North Korean counterparts.

In order to intercept transactions, an attacker needs to modify the computer code that runs an online store. HIDDEN COBRA managed to gain access to the store code of large retailers such as international fashion chain Claire's[7]. How HIDDEN COBRA got access is yet unknown, but attackers often use spearphishing attacks (booby-trapped emails) to obtain the passwords of retail staff.

Using the unauthorized access, HIDDEN COBRA injects its malicious script into the store checkout page. The skimmer waits for keystrokes of unsuspecting customers. Once a customer completes the transaction, the intercepted data - such as credit card numbers - are sent to a HIDDEN COBRA-controlled collection server.

Italian model agency as money mule

Curiously, HIDDEN COBRA used the sites of an Italian modeling agency and a vintage music store from Tehran to run its global skimming campaign.

To monetize the skimming operations, HIDDEN COBRA developed a global exfiltration network. This network utilizes legitimate sites, that got hijacked and repurposed to serve as disguise for the criminal activity. The network is also used to funnel the stolen assets so they can be sold on dark web markets. Sansec has identified a number of these exfiltration nodes, which include a modeling agency[8] from Milan, a vintage music store[9] from Tehran and a family run book store[10] from New Jersey.

Technical analysis

Sansec monitors millions of online stores for skimming activity and typically finds 30 to 100 infected stores per day. Many cases have a common modus operandi, such as shared infrastructure or striking features in programming style. These traits can be obvious, such as the debug message "Success bro" that led to the arrest of three Indonesians in December[6]. However, sometimes they are more subtle, as is the case with HIDDEN COBRA.

Sansec research has identified multiple, independent links between recent skimming activity and previously documented North Korean hacking operations. The following diagram shows (a small subset of) victim stores

The first campaign: clienToken=

```
<script src="https://www.luxmodelagency.com/wp-includes/js/customize-gtag.min.js"></script>
```

On June 23rd, 2019, Sansec discovered a skimmer on a US truck parts store that uses a compromised Italian modeling site[11] to harvest payment data. The injected script `customize-gtag.min.js` [12] is scrambled with a popular Javascript obfuscator[13]. Hidden in the code, the string `WTJ4cFpXNTBWRzlyWlc0OQ==` is found, which is the double-base64 encoded representation of `clientToken=`. This particular keyword is later used as HTTP GET parameter to send the stolen payload to the collector exfiltration node. The specific encoding and the attempt to disguise the stolen payload as "clientToken" form a uniquely identifying characteristic.

The malware was removed within 24 hours but a week later, the very same malware resurfaced on the same store. This time, it used a New Jersey book store to harvest credit cards[14]:

```
<script src="https://www.signedbooksandcollectibles.com/js/gmaps.min.js"></script>
```

During the following months, Sansec discovered the same malware on several dozen stores. Each time, it uses one of these hijacked sites as loader and card collector:

```
stefanoturco.com (between 2019-07-19 and 2019-08-10)
technokain.com (between 2019-07-06 and 2019-07-09)
darvishkhan.net (between 2019-05-30 and 2019-11-26)
areac-agr.com (between 2019-05-30 and 2020-05-01)
luxmodelagency.com (between 2019-06-23 and 2020-04-07)
signedbooksandcollectibles.com (between 2019-07-01 and 2020-05-24)
```

The second campaign: __preloader

In February and March 2020, several domain names were registrered that closely resemble popular consumer brands:

```
2020-02-10 PAPERS0URCE.COM
2020-02-26 FOCUSCAMERE.COM
2020-03-21 CLAIRES-ASSETS.COM
```

Subsequently, Sansec found the web stores of the three corresponding brands compromised with payment skimming malware installed. The anonymously registered domains were used as loader and card collector[15]

particularly odd code snippet, that Sansec has not observed anywhere else. The three relevant malware segments are displayed below for reference. Common behavior: upon form submission a hidden, dynamic image is added to the page with the deceptive name `__preloader`. The image address is controlled by the attacker, and the intercepted and encoded payload is sent as argument to this image, along with several random numbers. Immediately, the dynamic image is removed from the page, so the theft is invisible to the customer. Sansec has previously discussed this exfiltration method when it first reported on the Claire's hack on June 15th[7].

(code slightly modified for readability)

The common code, behavior, registrar and DNS server are unique traits that link these cases to the same source.

The North Korean link

As the diagram above shows, Sansec has established multiple, independent links to previously documented North Korean hacking activity. We will discuss each link separately.

technokain.com

South Korea based EST Security has published two articles[16] [17] documenting a North Korea-attributed attack where a malicious loader is embedded in Korean office documents. The loader installs remote access software for Windows on the victim's computer, which is downloaded from this address:

```
2019-07-12 https://technokain.com/ads/adshow1.dat
```

Additionally, US-based security firm Rewterz reported a spearphishing attack targeting attendees of the annual Consumer Electronics Show in Las Vegas[18]. This attack uses malware from the same address.

These attacks took place on July 11 and 12th, less than a week after the placement of a skimmer on the same site:

```
2019-07-06 https://technokain.com/vendor/jquery.validate.min.js
```

darvishkhan.net

Both Fortiguard Labs[19] and EST Security[20] document a DPRK-attributed spearphishing campaign that took place between June 26th and July 2nd 2019. The campaign used malicious Korean office documents

```
2019-06-27 https://darvishkhan.net/wp-content/uploads/2017/06/update6.dat
```

Two weeks earlier, multiple digital skimmers were launched from the same site, harvesting credit cards from several US, UK and Australia-based stores:

```
2019-06-12 https://darvishkhan.net/wp-includes/js/hotjar.min.js
2019-06-14 https://darvishkhan.net/wp-includes/js/dist/gtm.min.js
```

areac-agr.com

On October 25, Beijing-based Netlab360 discovered a novel remote access trojan (RAT) that showed multiple similarities with previously DPRK attributed malware[21]. Components of the tool were loaded from

```
2019-10-25 http://www.areac-agr.com/cms/wp-content/uploads/2015/12/check.vm
```

Before and after the presence of this malware, digital skimmers were hosted on the same site, that would intercept payments from multiple American stores:

```
2019-08-16 https://www.areac-agr.com/cms/wp-includes/Requests/Security1.3.min.js
2020-05-01 https://www.areac-agr.com/cms/wp-includes/Requests/Utility/json.min.js
```

papersOurce.com

The three malware domains from the `__preloader` campaign use distinct IPs. One of them - `papers0urce.com` - uses an address from Dutch ISP Leaseweb, `23.81.246.179`. This IP is not known to have been used for other domain names since 2015[22], however, it is featured in the same North Korea research as the previously discussed `areac-agr.com` [21]. The IP is hardcoded in the RAT, and used as a command and control (C2) server.

Discussion

Does the usage of common loader sites, and the similarity in time frame, prove that the DPRK-attributed operations are run by the same actor as the skimming operations? Theoretically, it is possible that different nefarious actors had simultaneous control over the same set of hijacked sites, but in practice, this would be extremely unlikely. First, thousands of sites get hacked each day[23], making an overlap highly coincidental. Secondly, when a site gets hacked, it is common practice for a perpetrator to close the exploited vulnerability after gaining access, in order to shield the new asset from competitors.

Conclusion

actors have engaged in large scale digital skimming activity since at least May 2019.

References

1. https://www.us-cert.gov/hiddencobra ↩
2. https://www.cyberscoop.com/north-korea-sanctions-lazarus-group-treasury-department/ ↩
3. https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX ↩
4. https://sansec.io/what-is-magecart ↩
5. https://sansec.io/research/magento-bruteforce-dashboard ↩
6. https://sansec.io/research/magecart-hackers-arrested ↩ ↩2
7. https://sansec.io/research/magecart-corona-lockdown ↩ ↩2
8. http://luxmodelagency.com/ ↩
9. https://www.darvishkhan.net/ ↩
10. https://www.signedbooksandcollectibles.com/ ↩
11. https://urlscan.io/result/e84b5381-4c24-4bff-b2f3-c600a07538d1/#transactions ↩
12. https://urlscan.io/responses/9fe97ae18c45e22fe76b8bd5165d0e152bec464d92ef5f7319b1723aba1c0edb/ ↩
13. https://obfuscator.io/ ↩
14. https://urlscan.io/result/18e3546d-8da0-49ac-9484-450a8ed90cd5/#transactions ↩
15. https://urlscan.io/result/f2052c0e-7df1-4b3a-b008-35476683a82f/#transactions ↩
16. https://blog.alyac.co.kr/2416 ↩
17. https://blog.alyac.co.kr/2418 ↩
18. https://www.rewterz.com/rewterz-news/rewterz-threat-alert-ces-themed-targeting-from-lazarus ↩
19. https://fortiguard.com/resources/threat-brief/2019/08/09/fortiguard-threat-intelligence-brief-august-09-2019 ↩
20. https://blog.alyac.co.kr/2397 ↩
21. https://blog.netlab.360.com/dacls-the-dual-platform-rat-en/ ↩ ↩2
22. https://www.virustotal.com/gui/ip-address/23.81.246.179/relations ↩
23. https://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/#135be6dd1738 ↩

Stay ahead of eCommerce hacks, protect your store today!

Sansec forensic experts were the first to document digital skimming in 2015. Since then, we have investigated thousands of hacked stores. Our research of the latest attack vectors protects our customers around the world. Our anti-skimming technology and data are used by merchants, forensic investigators, financial anti-fraud teams and service providers

Try our malware scanner

Stay up to date with the latest eCommerce attacks

E-mail address

Submit

Secure stores, happy shoppers