NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks

labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/

Juan Andrés Guerrero-Saade

SentinelLABS
NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks
By Juan Andrés Guerrero-Saade (JAGs)
READ BLOG >

Executive Summary

- In late May, 2021, Microsoft and Volexity released public reports detailing recent Nobelium activity.
- Nobelium is suspected to be the new face of APT29 (*aka* The Dukes). We track this activity under the name ‘NobleBaron’.
- This campaign employs a convoluted multi-stage infection chain, five to six layers deep.
- Most custom downloaders leverage Cobalt Strike Beacon in-memory as a mechanism to drop more elusive payloads on select victims.
- This report focuses on NobleBaron’s ‘DLL_stageless’ downloaders (*aka* NativeZone)
- SentinelLabs has discovered the use of one of these DLL_stageless downloaders as part of a poisoned update installer for electronic keys used by the Ukrainian government.
- At this time, the means of distribution are unknown. It’s possible that these update archives are being used as part of a regionally-specific supply chain attack.
- We uncovered additional unreported DLL_stageless downloaders.

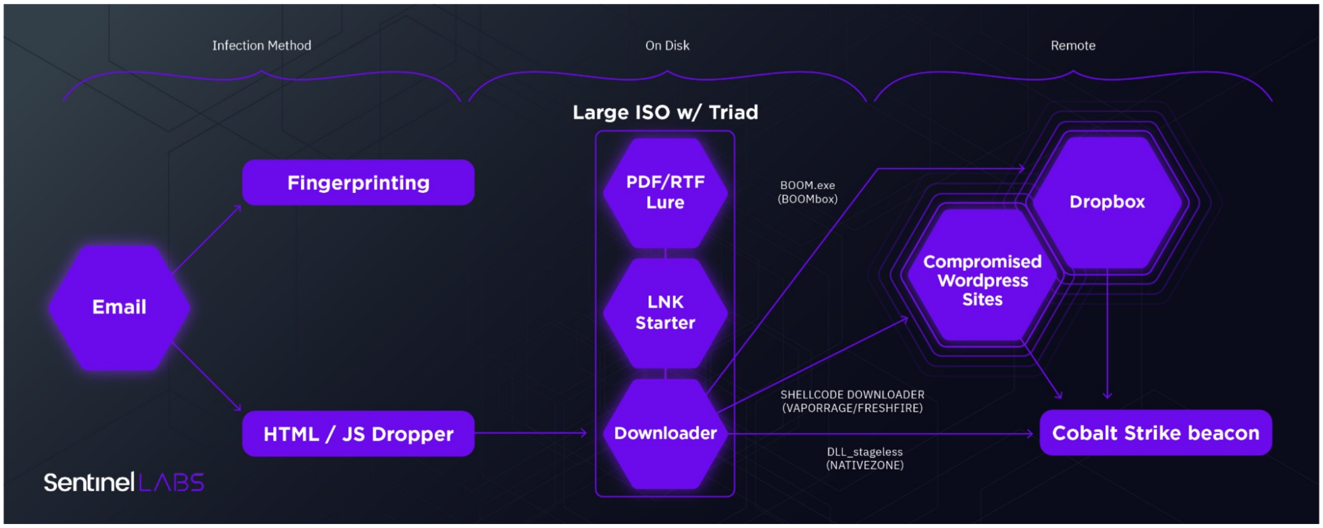
Overview

After the extensive revelations of Russian state-sponsored cyberespionage activities over the past five years, teams like APT28 (*aka* FancyBear, STRONTIUM) and APT29 (*aka* CozyBear, The Dukes) have retooled and reorganized extensively to avoid easy tracking by Western governments and security vendors alike. The operations of 'APT29' no longer look anything like they did in the past half decade. At this point our preconceptions about these groups are doing more to cloud our judgment than they elucidate. Perhaps new naming conventions (like 'NOBELIUM' or 'StellarParticle') will help piece these new clusters of activity apart– all the while upsetting folks who would prefer a simpler threat landscape than the one our reality affords us.

We track this new activity under the name 'NobleBaron', building off of the excellent reporting by Microsoft and Volexity. We acknowledge the suspicion that this is a newer iteration of APT29 but share in the general trepidation to equate the two. While the aforementioned companies have done excellent work exposing the inner workings of this activity, we wanted to contribute additional variants we encountered in our follow-on research, including a curious particularly insidious packaging of the 'NativeZone' downloader as part of a poisoned installer for a Ukrainian cryptographic smartkey used in government operations.

A Convoluted Infection Chain

As noted by Microsoft, the actor appears to be experimenting with various multi-stage infection chains. Common variations include the method of delivering the ISO containers and a wide variety of custom downloaders enmeshed with Cobalt Strike Beacon. There's a vague mention of an iOS zero-day being hosted on Nobelium fingerprinting servers but no mention as to whether this entails an iOS payload. That said, we also suspect no company is in a position to monitor iPhone endpoints for these payloads, Apple included.



While the Cobalt Strike Beacon payload is a disappointingly ubiquitous end for such a convoluted infection chain, it's not in fact the end of that chain. Rather, it serves as an early scout that enables selective distribution of rarer payloads directly into memory where they're less likely to be detected. A similar technique was employed by HackingTeam's Remote Control System (RCS) where initial infections used their 'Scout' malware for initial recon and could then be selectively upgraded to the full 'Elite' payload. After years of burned iterations on custom toolkits, it seems NobleBaron has opted for maximizing return on investment by simply lowering their upfront investment.

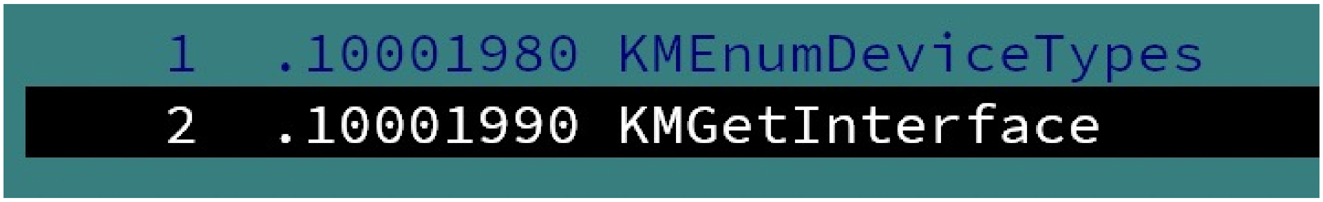
Notable TTPs include the following:

- An increasing depth in multi-layer droppers (a concept briefly described by Steve Miller and worth exploring further) particularly with regard to the inevitable CS Beacon payload.
- The use of large size files to avoid detection by security solutions with hardcoded size limits for 'efficiency'.
- A fishing-with-dynamite approach to collecting initial access to victims with low-cost tooling. The SolarWinds supply chain attack is one such example of starting with a wide victim pool and whittling down to high-value targets.

A Curious Poisoned Installer

SHA256
3b94cc71c325f9068105b9e7d5c9667b1de2bde85b7abc5b29ff649fd54715c4
SHA1
fc781887fd0579044bbf783e6c408eb0eea43485
MD5
66534e53d8751a24a767221fed01268d
Compilation Timestamp
2021-05-18 10:21:20
First Submission
2021-05-18 13:26:14
Size
282KB
Internal Name
KM.FileSystem.dll
File Description
IIT Бібліотека роботи з НКІ типу: "файлова система" (Ukrainian)

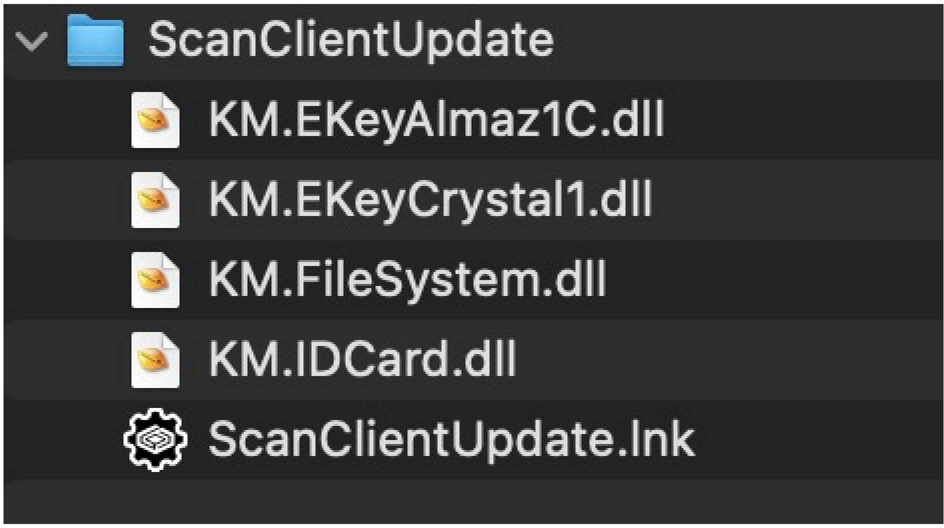
Most notably, one of these NativeZone downloaders is being used as part of a clever poisoned installer targeting Ukrainian government security applications. A zip file is used to package legitimate components alongside a malicious DLL (`KM.Filesystem.dll`). The malicious `KM.Filesystem.dll` was crafted to impersonate a legitimate component of the Ukrainian Institute of Technology's cryptographic keys of the same name. It even mimics the same two exported functions as the original.



```
1   .10001980 KMEnumDeviceTypes
2   .10001990 KMGetInterface
```

KM.Filesystem.dll exported functions

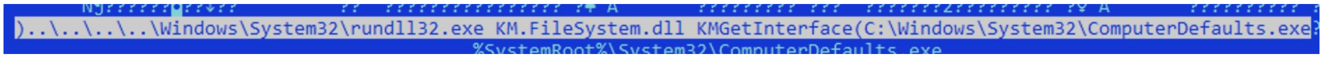
The package is not an ISO, but it follows a familiar formula. ‘ScanClientUpdate.zip’ relies on a triad of sorts. An LNK is used to kick off the malicious `KM.FileSystem.dll` component. In turn, `KM.FileSystem.dll` starts by checking for presence of `KM.EkeyAlmaz1C.dll` (a benign DLL). This check is presumably meant as an anti-sandbox technique that would keep this downloader from executing unless it’s in the same directory as the other packaged components.



```
ScanClientUpdate
    KM.EKeyAlmaz1C.dll
    KM.EKeyCrystal1.dll
    KM.FileSystem.dll
    KM.IDCard.dll
    ScanClientUpdate.lnk
```

ScanClientUpdate.zip contents

We stop short of referring to this as a supply chain attack since we lack visibility into its means of distribution. The poisoned installer may be delivered directly to relevant victims that rely on this regional solution. Alternatively, the attackers may have found a way of abusing an internal resource to distribute their malicious ‘update’.

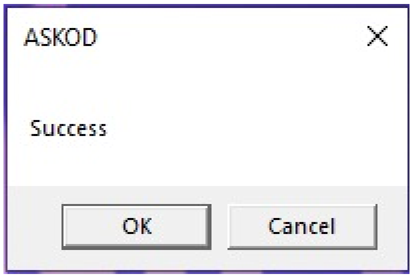


```
)..\..\..\..\Windows\System32\rundll32.exe KM.FileSystem.dll KMGetInterface(C:\Windows\System32\ComputerDefaults.exe
                    %SystemRoot%\System32\ComputerDefaults.exe
```

LNK starter command to run the malicious DLL

The LNK starter invokes the `KMGetInterface` export to execute the malware’s functionality. It passes a benign Windows component as an argument (`ComputerDefaults.exe`). The attackers will use the file’s attributes later on.

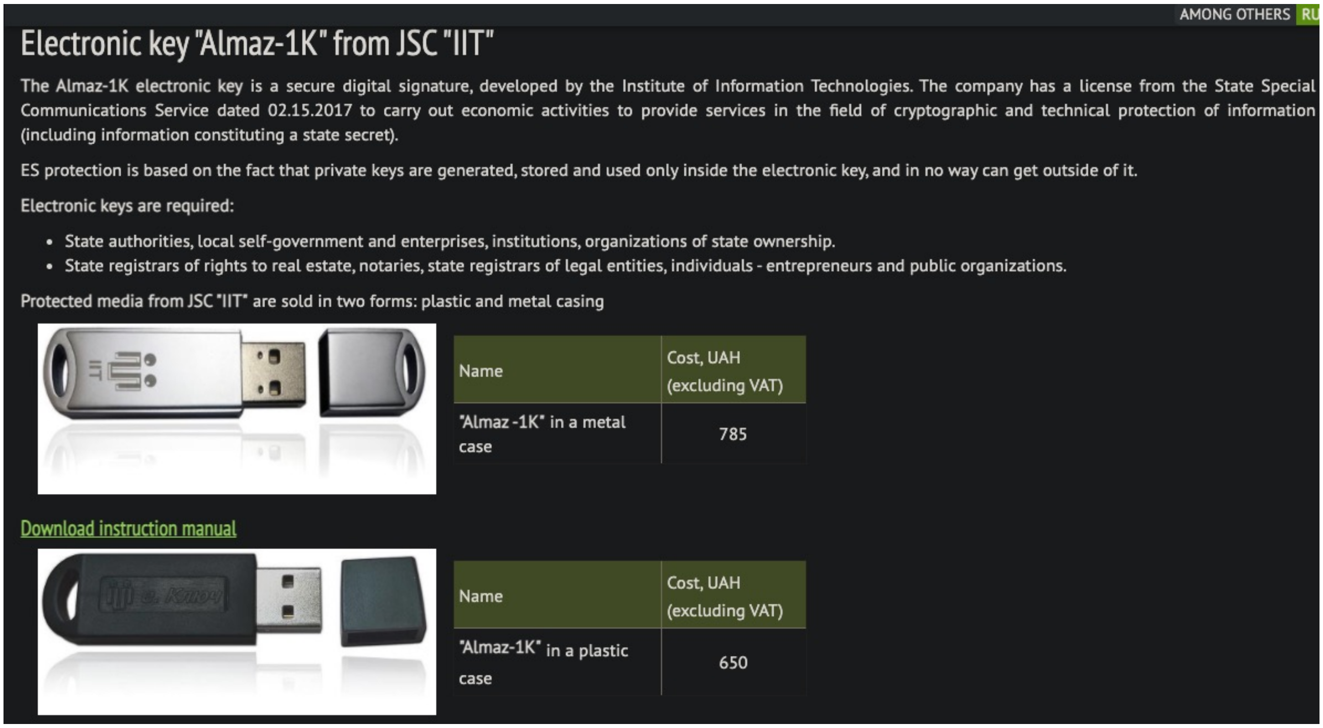
Upon execution, the user is presented with a vague ‘Success’ message box.



ASKOD

Success

Note that the heading of the message box is ‘ASKOD’, a reference to the Ukrainian electronic document management system. This initiative is meant to enforce electronic digital signatures through the use of cryptographic keys like the Алмаз-1К (transliterated as ‘Almaz-1K’ or translated to ‘Diamond-1K’) shown below.



Electronic key "Almaz-1K" from JSC "IIT"

The Almaz-1K electronic key is a secure digital signature, developed by the Institute of Information Technologies. The company has a license from the State Special Communications Service dated 02.15.2017 to carry out economic activities to provide services in the field of cryptographic and technical protection of information (including information constituting a state secret).

ES protection is based on the fact that private keys are generated, stored and used only inside the electronic key, and in no way can get outside of it.

Electronic keys are required:

- State authorities, local self-government and enterprises, institutions, organizations of state ownership.
- State registrars of rights to real estate, notaries, state registrars of legal entities, individuals - entrepreneurs and public organizations.

Protected media from JSC "IIT" are sold in two forms: plastic and metal casing

Name	Cost, UAH (excluding VAT)
"Almaz -1K" in a metal case	785

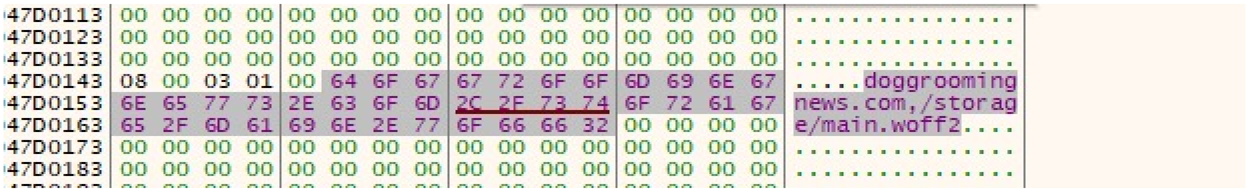
Download instruction manual

Name	Cost, UAH (excluding VAT)
"Almaz-1K" in a plastic case	650

Алмаз-1К electronic key description

These particular electronic keys are referenced in Ukrainian government tenders and make for a cunning regional-specific lure to distribute malware.

After displaying the message box, the malicious DLL proceeds to resolve APIs by hash and decrypts its payload directly into memory. You guessed it: Cobalt Strike Beacon v4.



```
47D0113 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
47D0123 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
47D0133 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
47D0143 08 00 03 01 00 64 6F 67 67 72 6F 6F 6D 69 6E 67 .....doggrooming
47D0153 6E 65 77 73 2E 63 6F 6D 2C 2F 73 74 6F 72 61 67 news.com,/storag
47D0163 65 2F 6D 61 69 6E 2E 77 6F 66 66 32 00 00 00 00 e/main.woff2....
47D0173 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
47D0183 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

It then decrypts the configuration via single-byte XOR `0x2E` and attempts to establish contact with the command-and-control server `doggroomingnews[.]com` . It checks for `‘/storage/main.woff2’` and if necessary falls back to `‘/storage/page.woff2’` . The domain resolves to an IP address in Ukraine (`45.135.167.27`), which appears to be a compromised domain.

While we have not been able to fetch the response at this time, it’s worth noting that this same IP was also contacted by a Cobalt Strike Beacon sample in late 2020:

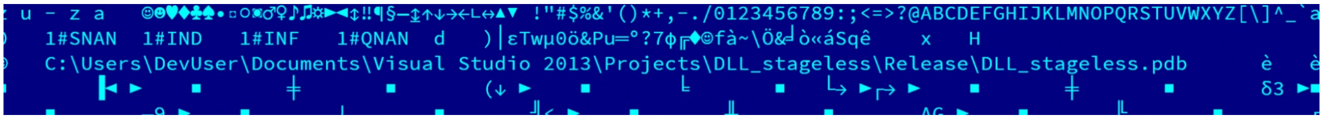
```
5a9c48f49ab8eaf487cf57d45bf755d2e332d60180b80f1f20297b16a61aa984 artifact.exe
```

These malicious updates are distributed in zip archives. At this time, we’ve discovered two ‘ScanClientUpdate.zip’ samples, both containing the same malicious DLL:

```
51b47cd3fc139e20c21897a00ac4e3b096380f939633233116514a1f2d9e63d5
ca66b671a75bbee69a4a4d3000b45d5dc7d3891c7ee5891272ccb2c5aed5746c
```

‘DLL_stageless’ (NativeZone) Variants

NobleBaron developers internally refer to these components under the name ‘DLL_stageless’



```
 u - z a   ☺☻♥♦♣♠•◘○◙♂♀♪♫☼►◄↕‼¶§▬↨↑↓→←∟↔▲▼ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`a
   1#SNAN  1#IND   1#INF   1#QNAN  d    )│εTwµ0ö&Pu═°?7ϕ╔♦☺fà~\Ö&┘ò«áSqê    x   H
   C:\Users\DevUser\Documents\Visual Studio 2013\Projects\DLL_stageless\Release\DLL_stageless.pdb      è   è
```

DLL_stageless PDB path

The following are variants of DLL_stageless with their respective delivery mechanisms and encrypted command-and-control configuration.

```
SHA256
2a352380d61e89c89f03f4008044241a38751284995d000c73acf9cad38b989e
SHA1
6114655cf8ddfd115156a1c450ba01e31887fabb
MD5
77605aa6bd6fb890b9b823bd7a3cc78b
Compilation Timestamp
2021-03-15 18:32:47
First Submission
2021-04-01 14:06:27
Size
299.50KB
ITW Name
MsDiskMountService.dll
Malicious Export
DiskDriveIni
C&C
74d6b7b2.app.giftbox4u[.]com
```

SHA256

776014a63bf3cc7034bd5b6a9c36c75a930b59182fe232535bb7a305e539967b

SHA1

247a32ebee0595605bab77fc6ff619f66740310b

MD5

e55d9f6300fa32458b909fded48ec2c9

Compilation Timestamp

2021-03-22 08:51:41

First Submission

2021-03-22 20:39:52

Size

351.50KB

ITW Name

diassvcs.dll

Malicious Export

InitializeComponent

C&C

content.pcmsar[.]net

SHA256

a4f1f09a2b9bc87de90891da6c0fca28e2f88fd67034648060cef9862af9a3bf

SHA1

19a751ff6c5abd8e209f72add9cd35dd8e3af409

MD5

600aceaddb22b9a1d6ae374ba7fc28c5

Compilation Timestamp

2021-02-17 13:18:24

First Submission

2021-02-25 16:33:09

Size

277KB

ITW Name

GraphicalComponent.dll

Malicious Export

VisualServiceComponent

C&C

139.99.167[.]177

Analyzing `GraphicalComponent.dll` led to the discovery of another DLL_stageless sample. At this time, we have not discovered the delivery mechanism. The name suggests the possibility of a different poisoned installer, with a focus on the Java SRE runtime.

SHA256
c4ff632696ec6e406388e1d42421b3cd3b5f79dcb2df67e2022d961d5f5a9e78
SHA1
95227f426d8c3f51d4b9a044254e67a75b655d6a
MD5
8ece22e6b6e564e3cbfb190bcbd5d3b9
Compilation Timestamp
2020-10-02 07:51:09
First Submission
2020-12-16 14:48:01
Size
277.50KB
ITW Name
Java_SRE_runtime_update.dll
Malicious Export
CheckUpdteFrameJavaCurrentVersion
C&C
hanproud[.]com

The malicious functionality of this sample is launched via the exported function `CheckUpdteFrameJavaCurrentVersion`. This particular instance of DLL_stageless doesn't check for a nearby file or specific directory.

References

https://twitter.com/MalwareRE/status/1398394028127932416
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/