The BLINDINGCAN RAT and Malicious North Korean Activity

sentinelone.com/blog/the-blindingcan-rat-and-malicious-north-korean-activity/

August 31, 2020

There has been a great deal of coverage lately around malicious activities attributed to North Korea (and/or adjacent entities). Most recently, this has culminated in the release of MAR (Malware Analysis Report) AR20-232A, which covers activities associated with the BLINDINGCAN RAT. This tool is the latest in a very long line of tools which allow attackers to maintain access to target environments as well as establish ongoing control of infected hosts. In this post, we give an overview of this campaign in context of other related campaigns, describing its infection vector, execution and high-level behavior.

Infection Vector

As we know, email phishing attacks are still the dominant method of delivering malware when it comes to these types of attacks. The BLINDINGCAN campaigns are no different, but their phishing lure comes with an interesting twist: malicious documents utilized in the campaign masquerade as job offers and postings from high-value defense contractors such as Boeing.

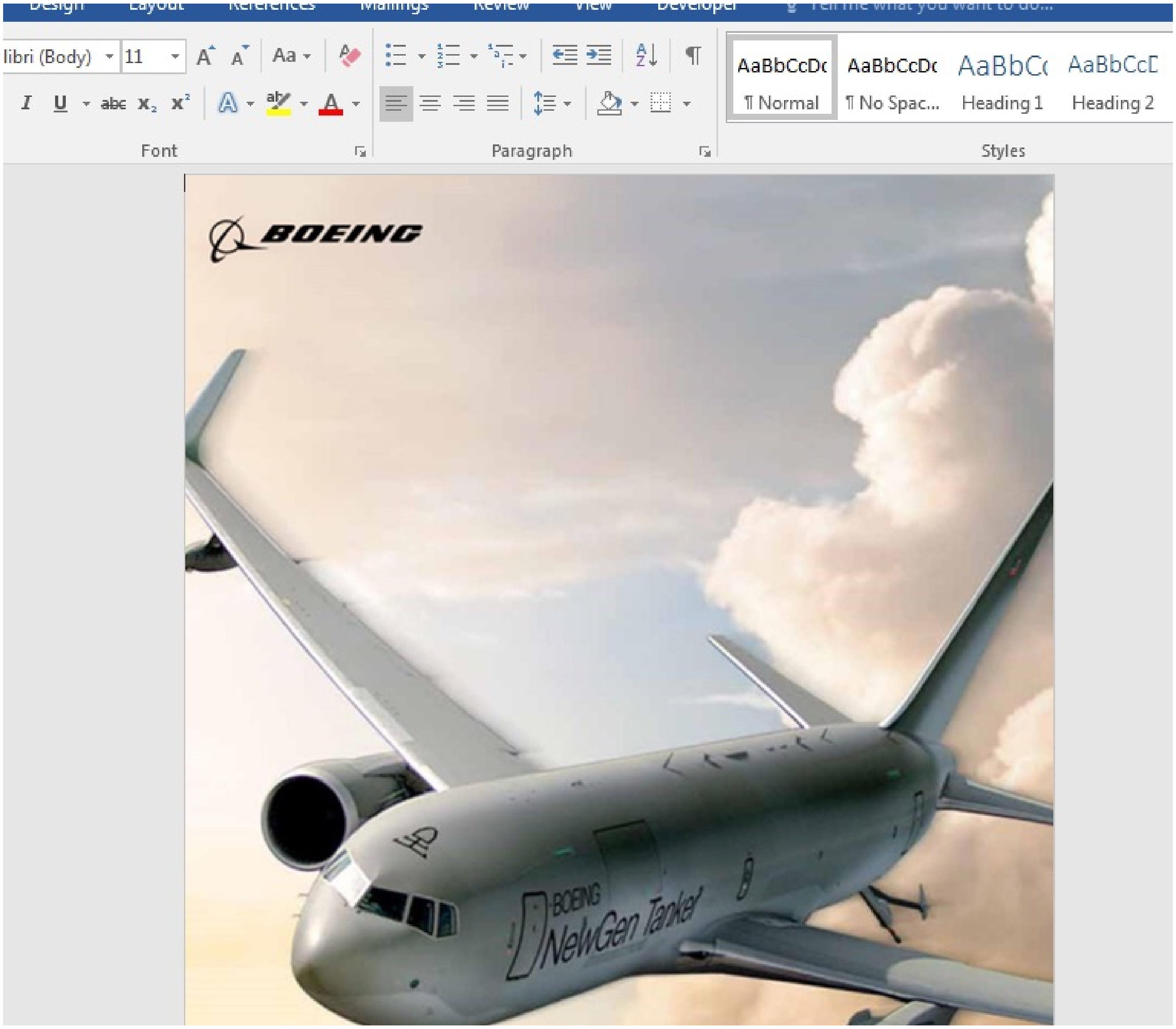
This isn’t the first time such a lure has been used. Sophisticated attackers have sought to mimic entities in the defense, military, and government space in the past. This is especially true, historically, with campaigns tied to North Korea. Even early on in 2020, Operation North Star followed a very similar modus operandi, and by some accounts these campaigns may be related.

CISA maintains a running repository of North Korean / Hidden Cobra related advisories and details. Their alerts cover campaigns from 2017 to present, including (but not limited to):

- WannaCry – Massively destructive “ransomware” with SMB spreading capabilities.
- Delta Charlie – Backdoor and Denial-of-Service tool set
- Volgmer – Backdoor
- FALLCHILL – Full-function RAT
- BANKSHOT – RAT and proxy/tunneling tool set
- HARDRAIN – RAT and proxy tool set w/ Android support
- SHARPKNOT – MBR Wiper
- TYPEFRAME – RAT and proxy/tunneling tool set
- KEYMARBLE – Full-function RAT
- FASTCash – RAT and proxy/tunneling tool set (Financial attacks)

- BADCALL – RAT and proxy tool set w/ Android support
- ELECTRICFISH – proxy/tunneling tool set
- HOPLIGHT – proxy/tunneling tool set with pseudo-SSL spoofing
- ARTFULPIE – Downloader and launcher tool set
- CROWDEDFLOUNDER – Full-function RAT
- TAINTEDSCRIBE – Downloader and launcher with LFSR (LInear Feedback Shift Register) support
- COPPERHEDGE – Full-function RAT, cryptocurrency and crypto-exchange focused.

In short, the DPRK has a long history of these types of campaigns and it does not appear to be letting up in frequency or aggressiveness. Moreover, North Korea is no stranger to playing the ‘long-game’. Reflecting back on earlier attacks from the region (e.g., Operation Troy, Ten Days of Rain, Dark Seoul, and the Sony attack) we see similar tactics and aggressiveness.



The BLINDINGCAN campaign has been specifically focused on defense and aerospace targets, primarily based in Europe and the United States. According to AR20-232a: “The FBI has high confidence that HIDDEN COBRA actors are using malware variants in conjunction with proxy servers” along with “compromised infrastructure from multiple countries to host its command and control (C2) infrastructure”.

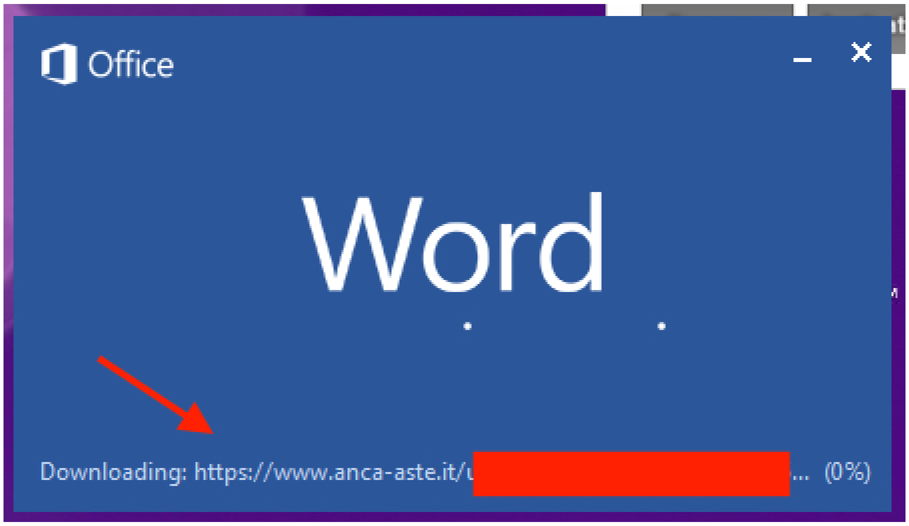
The objective of these attacks is to gain intelligence and to understand the key technologies that fall under the umbrella of the targeted entity, as well as those adjacent to them (contactors, partners, etc.)

BLINDINGCAN RAT: Execution and Behavior

The malicious documents themselves, upon launch, attempt to exploit CVE-2017-0199. This particular flaw allows for remote code execution via maliciously crafted documents. More specifically, CVE-2017-0199 is a result of the flawed processing of RTF files and elements by way of a potent combination of object links and HTA payloads.

This vulnerability is a common vector of attack for malicious actors, and despite the flaw being patched long ago, attackers bet on the fact (often successfully) that at least some of their targets will still be exposed to the flaw, allowing them to achieve their foothold.

You can see this behavior immediately upon launching one of the malicious documents.



Downloading: https://www.anca-aste.it/[redacted]... (0%)

The samples we analyzed reach out to a remote server (C2) for additional components. Once established, a keylogging and clipboard monitoring component is dropped, and additional information is extracted from the targeted hosts. WMI commands are utilized to gleen basic system details:

```
start iwbemservices::execquery - select * from win32_computersystemproduct
```

The RAT component (e.g., `58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d`) can be found in both 32 and 64 bit varieties. The executable payloads employ multiple levels of obfuscation.

Configuration data for the RAT is embedded in the payloads and is both encrypted and encoded. Embedded configuration artifacts are AES-encrypted with a hard-coded key. Upon decrypting, the resulting data is then decoded via XOR. Strings in the malware are RC4 encrypted.

The RAT module will initially pull basic system data. The aforementioned WMI command is part of this system reconnaissance process. In this stage, the malware will pull local network data, system name, OS version details, processor/platform details and MAC address details, and then push this data to the C2.

The core RAT feature set boils down to the following:

- Gather and transmit defined set of System features
- Create, terminate and manipulate processes
- Create, terminate and manipulate files
- Self-updating / self-deletion (cleaning of malicious code from the system when necessary)

Conclusion

While the malware and implants discussed here are specific to operations attributed to North Korea, the delivery and weaponization states are common to most other APT groups and non-nation-state backed campaigns.

The key takeaways here are 1) it is important to keep abreast of the evolution of malicious attacks generated from this region, but also 2) we can apply what we have learned from other past attacks to improve our posture and reduce overall exposure, along with the potential negative repercussions of suffering from such an attack. Prevention, as always, is key. The SentinelOne Singularity Platform is fully capable of detecting and preventing malicious activity associated with HIDDEN COBRA and BLINDINGCAN.

Indicators of Compromise

SHA256
6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1
8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050
58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d
7933716892e0d6053057f5f2df0ccadf5b06dc739fea79ee533dd0cec98ca971

SHA1

0ecc687d741c7b009c648ef0de0a5d47213f37ff
3f6ef29b86bf1687013ae7638f66502bcf883bfd
9feef1eed2a8a5cbfe1c6478f2740d8fe63305e2
C70edfaf2c33647d531f7df76cd4e5bb4e79ea2e

Domains

agarwalpropertyconsultants[.]com
curiofirenze[.]com
automercado.co[.]cr

MITRE ATT&CK

Phishing: Spearphishing Attachment [T1566]
Command and Scripting Interpreter: PowerShell [T1059]
Exploitation for Client Execution [T1203]
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547]
Process Injection [T1055]
Deobfuscate/Decode Files or Information [T1140]
System Time Discovery [T1124]
Account Discovery [T1087]
Query Registry [T1012]
Process Discovery [T1424]
System Owner/User Discovery [T1033]
Automated Collection [T1119
Data from Local System [T1533]]
Remote File Copy [T1544
Automated Exfiltration [T1020]]
Exfiltration Over C2 Channel [T1041]