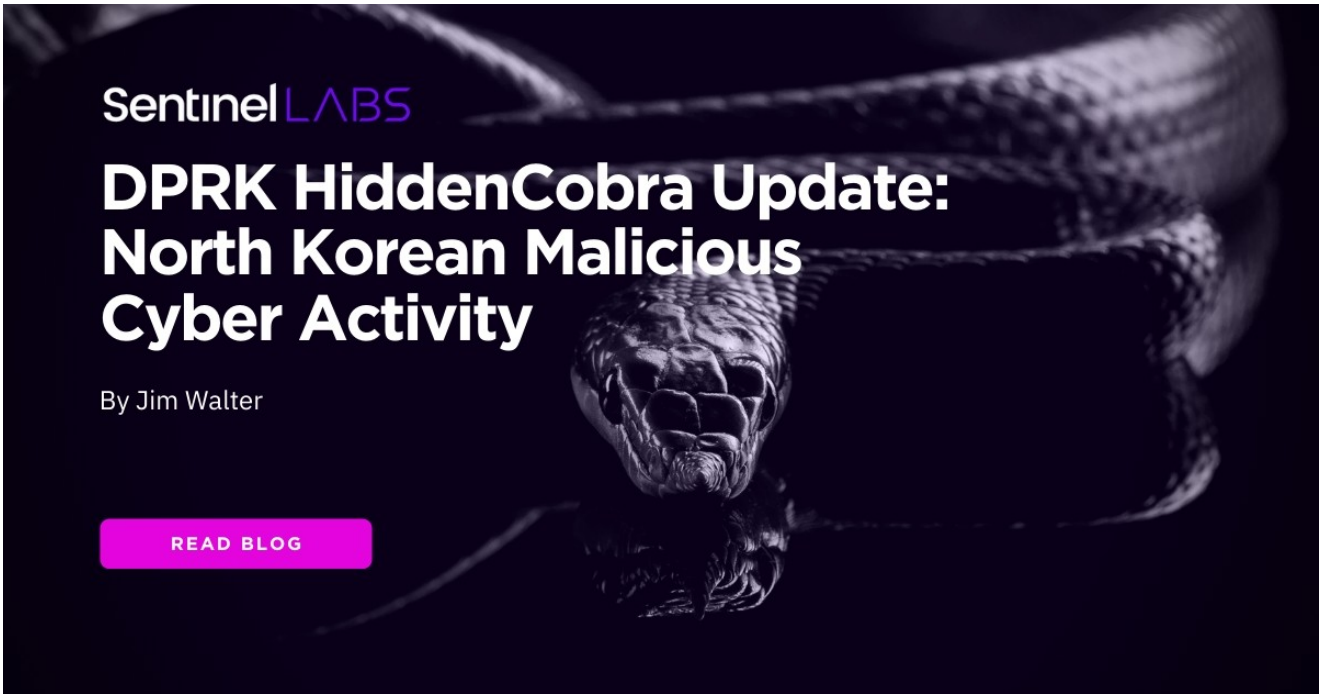
DPRK Hidden Cobra Update: North Korean Malicious Cyber Activity

labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/

Jim Walter



North Korea (specifically the Lazarus group) has a long and storied history of destructive cyber-attacks. Some more notable examples are the 2013 “Dark Seoul” attacks, the 2014 attack on Sony Pictures, a series of SWIFT-targeted campaigns in 2015-2016, and more recently their foray into commercial cybercrime operations with Trickbot and Anchor.

The US-CERT recently released a new set of MARs (Malware Analysis Reports) covering newly uncovered/updated malware/implants attributed to North Korea. More specifically, these are tools attributed to the Lazarus Group / Hidden Cobra. These updates provide a sizeable glimpse into the ever expanding DPRK toolset. As we have seen in the past, the complexity and sophistication of these tools varies widely. Most of the families covered in this update are meant to function as RATs or Cobalt-Strike-like (beacon) tools meant to enable persistence and manipulation of infected hosts.

BISTROMATH

Full Featured RAT (Remote Access Trojan) payloads and associated CAgent11 implant builder/controller. This implant is used for standard system management, control and recon. Initial infection is carried out via a malicious executable. An embedded bitmap image (contained in the trojan) is decoded into shellcode upon execution, thus loading the implant.

Network communications are encrypted via XOR. The analyzed BISTROMATH samples, along with the other families all attempt to evade analysis via common sandboxes (VIRTUALBOX, QEMU, VMware) via multiple artifact checks (presence of specific devices, registry entries, processes, files).

Core functionality includes:

· File and Process manipulation
· File/Data upload/exfiltration
· Timestamp modification/masquerading
· Service start/stop
· CMD shell access / use
· Screenshot Capture
· Microphone Capture
· Webcam Control
· Keylogging
· Browser hijacking/form grabbing
· Exfiltration of cached credentials
· Self-management (update/uninstall)

HOPLIGHT

Proxy payload to obfuscate and/or re-route traffic between infected hosts and C2. Traffic is encrypted over SSL, and the individual payloads are capable of generating fake SSL Certificates. Analyzed samples are Themida packed. One of the examples (SHA256: d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39) provided by CISA contained a public SSL certificate and encrypted payload.

SLICKSHOES

SLICKSHOES is typically utilized as a loader/Dropper. The malware writes itself to “C:WindowsWebtaskenc.exe”. Separate processes are responsible for the manipulation and execution of the dropped executable. SLICKSHOES is a full beacon-style implant (similar to Cobalt Strike).

Makes use of bespoke encoding methods and is capable of RAT-like functionality.

· File and Process manipulation
· System recon and exfiltration
· Input capture
· Command/process execution and manipulation

SLICKSHOES communicates to a hardcoded C2 address (188[.]165[.]37[.]168) on TCP port 80. Communication occurs in 60-second intervals.

CROWDEDFLOUNDER

CROWDEDFLOUNDER functions as a memory-resident RAT (32-bit and Themida packed). The malware accepts arguments at runtime, and can be installed as a service.

CROWDEDFLOUNDER implants can perform full two-way comms with C2, however in context the primary function appears to be a proxy for inbound connections from the C2. Upon execution the malware will manipulate local firewall settings to allow for flow of its traffic. C2 traffic and data transfers are encrypted via rotating XOR.

Functionality includes:

· File and Process manipulation
· System recon and exfiltration
· Input capture
· Command/process execution and manipulation

HOTCROISSANT

HOTCROISSANT is a full beacon-style (Cobalt Strike style) implant with RAT-like functionality. Network traffic is encoded via XOR. C2 communications are limited to a hard-coded IP (94.177.123.138:8088). Upon infection, victim information is transferred to the C2. After this point, the malware listens and responds to commands from the C2.

ARTFULPIE

ARTFULPIE is responsible for retrieval and injection of a DLL-based payload. The malware contains a hard-coded URL from which to download the additional code (193[.]56[.]28[.]103).

BUFFETLINE

BUFFETLINE is a full, beacon-style, implant with RAT-like functionality.

Features include:

· File and Process manipulation
· System recon and exfiltration
· CLI status manipulation
· Lateral targeting & enumeration
· Command/process execution and manipulation

Analyzed samples utilize a combination of RC4 encoding and PolarSSL (auth) to obfuscate network communications. Once authenticated to the C2, the trojan will send a collection of victim information and then await further interaction.

Data transferred includes:

· Victim “ID”
· Implant Version
· System directory location
· Hardware details (network adapters, CPU revision)
· OS Version / Software environment data
· Computer Name
· Victim IP Address

Conclusion

Adversarial toolsets are constantly evolving. The upper tier of sophisticated, or state-backed threats, have rapid and agile development/release cycles, mirroring the world of legitimate software development. Staying on top of these trends is a critical piece of protecting our environments against these threats. A power and modern security platform (ex: SentinelOne Singularity) is required to tackle these evolving threats from both static and behavioral angles.

IOCs

HOPLIGHT

SHA-256: 05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461
SHA-256: 0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571
SHA-256: 084b21bc32ee19af98f85aee8204a148032ce7eabef668481b919195dd62b319
SHA-256: 12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d
SHA-256: 1a01b8a4c505db70f9e199337ce7f497b3dd42f25ad06487e29385580bca3676
SHA-256: 2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
SHA-256: 32ec329301aa4547b4ef4800159940feb950785f1ab68d85a14d363e0ff2bc11
SHA-256: 4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
SHA-256: 4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818
SHA-256: 70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
SHA-256: 73dcb7639c1f81d3f7c4931d32787bdf07bd98550888c4b29b1058b2d5a7ca33
SHA-256: 83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a
SHA-256: 8a1d57ee05d29a730864299376b830a7e127f089e500e148d96d0868b7c5b520
SHA-256: b05aae59b3c1d024b19c88448811debef1eada2f51761a5c41e70da3db7615a9
SHA-256: b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101
SHA-256: c66ef8652e15b579b409170658c95d35cfd6231c7ce030b172692f911e7dcff8
SHA-256: d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39
SHA-256: ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
SHA-256: f8f7720785f7e75bd6407ac2acd63f90ab6c2907d3619162dc41a8ffa40a5d03
SHA-256: fe43bc385b30796f5e2d94dfa720903c70e66bc91dfdcfb2f3986a1fea3fe8c5

112[.]175[.]92.57
113[.]114[.]117.122
117[.]239[.]241.2
119[.]18[.]230.253
128[.]200[.]115.228
137[.]139[.]135.151
14[.]140[.]116.172
181[.]39[.]135.126
186[.]169[.]2.237
195[.]158[.]234.60
197[.]211[.]212.59
21[.]252[.]107.198
210[.]137[.]6.37
217[.]117[.]4.110
218[.]255[.]24.226
221[.]138[.]17.152
26[.]165[.]218.44
47[.]206[.]4.145
70[.]224[.]36.194
81[.]94[.]192.10
81[.]94[.]192.147
84[.]49[.]242.125
97[.]90[.]44.200

ARTFULPIE

SHA-256: 606c6000f36dc69fefc6df828e1ac9c5529a71a62b99f5df55463606c4c9689c

193[.]56[.]28.103

HOTCROISSANT

SHA-256: 8ee7da59f68c691c9eca1ac70ff03155ed07808c7a66dee49886b51a59e00085

94[.]177[.]123.138

CROWDEDFLOUNDER
SHA-256: a2a77cefd2faa17e18843d74a8ad155a061a13da9bd548ded6437ef855c14442

SLICKSHOES
SHA-256: fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac

188[.]165[.]37.168

BISTROMATH
SHA-256: 04d70bb249206a006f83db39bbe49ff6e520ea329e5fbb9c758d426b1c8dec30
SHA-256: 1ea6b3e99bbb67719c56ad07f5a12501855068a4a866f92db8dcdefaffa48a39
SHA-256: 618a67048d0a9217317c1d1790ad5f6b044eaa58a433bd46ec2fb9f9ff563dc6
SHA-256: 738ba44188a93de6b5ca7e0bf0a77f66f677a0dda2b2e9ef4b91b1c8257da790

159[.]100[.]250.231

BUFFETLINE
SHA-256: 52f83cdaefd194fff3d387631d5693a709cd7b3a20a072e7827c4d4218d57695

107[.]6[.]12.135
210[.]202[.]40.35

MITRE ATT&CK

Lazarus Group – G0032
Commonly Used Port – T1043
Connection Proxy – T1090
Credential Dumping – T1003
Custom Cryptographic Protocol – T1024
Data Encoding – T1132
Data from Local System – T1005
Data Staged – T1074
Exfiltration Over Alternative Protocol – T1048
Exfiltration Over Command and Control Channel – T1041
File and Directory Discovery – T1083
Input Capture – T1056
New Service – T1050
Obfuscated Files or Information – T1027
Process Discovery – T1057
Process Injection – T1055
Query Registry – T1012
Registry Run Keys / Startup Folder – T1060
Remote File Copy – T1105
Scripting – T1064
Spearphishing Attachment – T1193
System Information Discovery – T1082
System Network Configuration Discovery – T1016
System Owner/User Discovery – T1033
System Time Discovery – T1124

Uncommonly Used Port – T1065
User Execution – T1204
Software: HOPLIGHT – S0376