New North Korean Malware Families Identified, Including Ransomware, Credential Harvester, and Others; Links to 'Andariel' Cluster

Fusion (FS) | Cyber Espionage (CE)

July 06, 2021 07:45:00 PM, 21-00014321, Version: 1

Executive Summary

- Mandiant Threat Intelligence identified several FINEART samples loading new malware tools, including a backdoor, port scanner, utility, and credential harvester, that we believe are attributable to a North Korean activity set that broadly aligns with the publicly reported "Andariel" cluster.
- The backdoor, dubbed "LOOKINGGLASS," shares code and infrastructure with ransomware first reported by Kaspersky and tracked internally as SHATTEREDGLASS.
- This activity presents a primary risk to defense and aerospace industries and a secondary risk to financial entities or other organizations perceived as lucrative targets for financially motivated operations.
- Please see the Technical Annex for YARA and Snort rules.

Threat Detail

Mandiant Threat Intelligence identified new malware families believed to be related to HIDDENGIFT, a backdoor employed in a suspected North Korean campaign in April 2021. The new tools were observed being loaded by FINEART and include a port scanner, credential harvester, utility, and a backdoor. Notably, the backdoor, dubbed "LOOKINGGLASS," shares infrastructure and callout similarities with ransomware first reported by Kaspersky and internally tracked as SHATTEREDGLASS.

- Mandiant identified several FINEART loaders that load the PAINTBRUSH port scanner, ARTCURATOR credential harvester, BLANKCANVAS utility, and LOOKINGGLASS backdoor.
- In April 2021, FINEART was observed decoding and loading HIDDENGIFT into memory in a campaign targeting the South Korean defense industry (21-00009443).
- SHATTEREDGLASS is not loaded via FINEART, but it sends the same callout, expects the same response, and uses the same infrastructure as the LOOKINGGLASS backdoor.
    - Mandiant cannot corroborate Kaspersky's indication that the ransomware has been used against a victim; we have not identified SHATTEREDGLASS being deployed against a victim.
- Many files are time-stomped, but the activity appears to span from late 2018 to early 2021 (please see the Technical Annex for more information).

Attribution

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.
FIIP ENVIRONMENTS ORGANIZATION
rebecca.heller@FireEye.com

We assess with moderate confidence that these new malware families are attributable to a North Korean activity set that broadly aligns with "Andariel"-related activity based on decode routine overlaps and targeting consistencies.

- While HIDDENGIFT has documented overlaps with TEMP[.]Hermit malware, it uses a unique decode routine only observed in IRONSMITH and ROGUEEYE malware, each of which are leveraged by tracked activity clusters associated with the broader Andariel cluster (20-00025799).
- Andariel-related activity sets have targeted the aerospace and defense industry; QUINSTATUS, for example, was leveraged against this sector in South Asia and the U.S. earlier in June (21-00013151).
- Mandiant detected LOOKINGGLASS activity at a South Korean defense and aerospace entity in June 2021.
- Public reporting by Kaspersky corroborates this activity's historical focus on South Korea. They also reported several victims including those in the manufacturing, home network service, media, and construction sectors, and that the ransomware was delivered to a target in at least one case.

Outlook and Implications

This activity's targeting and indications of financial motives via ransomware are consistent with North Korean efforts that conduct financially motivated activity alongside espionage operations. Further, the identification of new malware families aligns with the North Korean tempo of operations, which includes the continuous development of tools that exhibit shared resources or overlaps between groups (e.g., HIDDENGIFT and TEMP[.]Hermit). Mandiant believes that the identification of ransomware associated with this activity is representative of a secondary financially motivated effort supporting the identification of revenue streams to offset financial impacts related to sanctions and the coronavirus (COVID-19) pandemic, while the targeting of the aerospace and defense industry is likely a primary effort that aligns with North Korea's strategic objectives. Further, recent targeting campaigns may be driven by the recent lift of missile restrictions on South Korea.

Technical Annex

Mandiant Threat Intelligence identified several FINEART loaders related to previous HIDDENGIFT activity with at least one targeting the aerospace and defense industry. The loaders were observed loading backdoors HIDDENGIFT and LOOKINGGLASS as well as a port scanner PAINTBRUSH, credential harvester ARTCURATOR, and a utility BLANKCANVAS.

PAINTBRUSH Characteristics

PAINTBRUSH is a Windows port scanner capable of

- Accepting the destination from the command line
- Accepting the destination from a file on the fie system

ARTCURATOR Characteristics

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

ARTCURATOR is a Windows credential harvester capable of

- Collecting Office and HWP document history
- Collecting username and passwords from Chrome, Firefox, and Internet Explorer

BLANKCANVAS Characteristics

BLANKCANVAS is a Windows utility capable of

- Accepting a file from the command line
- Adding the file to a shortcut menu of another file

LOOKINGGLASS Characteristics

LOOKINGGLASS is a Windows backdoor capable of

- Keylogging
- Capturing screenshots
- Running arbitrary commands
- Reading and writing files

SHATTEREDGLASS Characteristics

SHATTEREDGLASS is Windows ransomware capable of

- Retrieving an encryption key from the C&C server
- Encrypted files
- Prompting the victim for payment

While HIDDENGIFT has overlap with TEMP[.]Hermit activity described in 21-00009443, it also uses a unique decode routine only observed in suspected Andariel activity, including IRONSMITH and ROGUEEYE. Additionally, recent suspected Andariel QUINSTATUS samples were observed also targeting the aerospace and defense industry as described in 21-00013151. Due to targeting and code re-use, Mandiant Threat Intelligence assesses that this activity is more related to Andariel and shows code and infrastructure sharing between the two groups.

During analysis another sample of previously reported SILVERFROG was identified targeting the aerospace and defense industry. SILVERFROG is loosely suspected to be TEMP[.]Hermit based on code similarities with NORTHFOOT. SILVERFROG may be used by Andariel or by TEMP[.]Hermit with a focus on targeting aerospace and defense.

The additional FINEART loaders mentioned in this report were discovered pivoting from the string "js9$_wR$3" found in one of the loaders. It is unclear why this string is present as it appears to not be used, but it is believed all the FINEART loaders are used by the same

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

actor. All of the loaders are time-stomped and some of them have the actual timestamp appended at the end of the file.

SHATTEREDGLASS Execution

UNAVAILABLE (MD5: d96fcd2159643684f4573238f530d03b)

- Timestamp: 2020-09-19T09:41:19Z
- Expects command line arguments
  - <DRIVE> <FLAG> <DATA 1> <DATA 2> <EMAIL> <FILENAME> <ID>

Argument	Description
<DRIVE>	Drive to encrypt
<FLAG>	Can be "-s", "-S", "-k", or "-K" The S flags specify a C&C server The K flags specify an encryption key
<DATA 1>	If S is provided: Encryption IV If K is provided: IP of C&C server
<DATA 2>	If S is provided: Encryption Key If K is provided: Port of C&C server
<EMAIL>	Contact email inserted into the ransom message
<FILENAME>	Uses this filename instead of 3nc004
<ID>	ID used for tracking

- If a C&C server was provided, calls out to perform a handshake
  - Send: HTTP 1.1 /member[.]php SSL3.4
  - Recv: HTTP 1.1 200 OK SSL2.1
- Receives the encryption key from the C&C server
- Encrypts files with the extension .3nc004
- Writes the ransom message to 3nc004[.]txt in %DESKTOP% and %STARTUP%
- Opens the message in notepad[.]exe
- Can uninstall itself with
- cmd[.]exe /C ping 1[.]1[.]1[.]1 -n 1 -w 3000 > Nul & Del /f /q <FILE>

LOOKINGGLASS Execution

UNAVAILABLE (MD5: 6e710f6f02fdde1e4adf06935a296fd8)

- Timestamp: 2021-01-11T05:57:28Z
- Contains code for the following
  - Keylogging
  - Screen capture
  - File management
  - Updating itself
  - Running commands
- C&C server: 45[.]58[.]112[.]77

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

ARTCURATOR Execution

UNAVAILABLE (MD5: c3cecb6c82be49658ba01872e0f643b9)

- ARTCURATOR credential harvester
- Timestamp: 2018-10-23T18:51:48Z
- Uses open source software (OSS) similar to browser-dumpwd
- Collects username and passwords, with the OSS, from
  - Firefox
  - Chrome
  - Internet Explorer
- Collects document history from
  - Hangul Office
  - Microsoft Word

PAINTBRUSH Execution

UNAVAILABLE (MD5: 2968c20a07cfc97a167aa3dd54124cda)

- PAINTBRUSH port scanner
- Timestamp: 2020-01-28T04:34:39Z
- Loaded by MD5 9a570c53b1a811aba02b2b76cc65b5eb
- Scans ports based off four arguments from the command line

Flag	Description
-h	Destination IP
-p	Port range
-f	Supplemental file of IPs and port ranges
-o	Output file

- Results are saved to a file as one of the following
  - <IP>:<PORT> -> OPENED!
  - <IP>:<PORT> -> CLOSED!

BLANKCANVAS Execution

UNAVAILABLE (MD5: f2132947d0668084620c7687342c7bb9)

- BLANKCANVAS utility
- Timestamp: 2019-06-05T11:09:06Z
- Takes a command as a command line argument
- Adds the command as a shortcut menu item to a file
  - It isn't clear how the command gets executed
- Registry entries are set to achieve the menu item
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
    - Default

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Default[.]exe
  - c:\\windows\\system32\\msdxm[.]tlb
- HKCU\SOFTWARE\Classes\.tlb
  - System[.]Collections[.]Logic[.]tlb
- HKCU\SOFTWARE\Classes\System[.]Collections[.]Logic[.]tlb\Shell\Open\Command
  - <COMMAND LINE ITEM>

Related Files

ARTCURATOR

FINEART loaders were identified loading ARTCURATOR.

ExeInfoPE[.]exe (MD5: fb60f04f65d169a4471129e171d6b88d)

- FINEART loader
- Timestamp: 1995-09-23T01:43:17Z
- Payload is RC4 encrypted
- Loads MD5 c3cecb6c82be49658ba01872e0f643b9

ExeInfoPE[.]exe (MD5: f22a09b3f55b2fbb788174e9c7e03825)

- FINEART loader
- Timestamp: 1999-05-08T16:28:37Z
- Payload is RC4 encrypted
- Loads MD5 c31e4e02aeeeae188f4404a8ad6d9f03

UNAVAILABLE (MD5: c31e4e02aeeeae188f4404a8ad6d9f03)

- ARTCURATOR credential harvester
- Timestamp: 2020-06-09T06:44:19Z
- This sample doesn't collect document history

PAINTBRUSH

A FINEART loader was identified loading PAINTBRUSH.

ExeInfoPE[.]exe (MD5: 9a570c53b1a811aba02b2b76cc65b5eb)

- FINEART loader
- Timestamp: 1995-09-23T01:43:17Z
- Loads MD5 2968c20a07cfc97a167aa3dd54124cda

BLANKCANVAS

A FINEART loader was identified loading BLANKCANVAS.

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

ExeInfoPE[.]exe (MD5: 779e53e6a0e08805617479d1f4ac4cca)

- FINEART loader
- Timestamp: 1995-09-23T01:43:17Z
- Loads MD5 f2132947d0668084620c7687342c7bb9

HIDDENGIFT

Other FINEART loaders containing HIDDENGIFT were identified.

UNAVAILABLE (MD5: f3fcb306cb93489f999e00a7ef63536b)

- FINEART loader
- Timestamp: 1996-04-05T00:15:49Z
- Time appended to file: Mon Apr 19 08:46:58 2021
- Payload is formatted as
  - <4-Byte Length><16-Byte XOR Key><XOR Encoded Data>
- XOR key: 556B6E654321313140324451 4B7843
- Only the first 15 bytes of the key is used
- Loads MD5 fdc66cdabd46bc3b26aba4e59943726b

UNAVAILABLE (MD5: fdc66cdabd46bc3b26aba4e59943726b)

- HIDDENGIFT backdoor
- Timestamp: 2020-12-13T04:14:17Z
- C&C servers:
  - hxxp://mail[.]neocyon[.]com/jsp/user/sms/sms_recv[.]jsp
  - hxxp://mail[.]sisnet[.]co[.]kr/jsp/user/sms/sms_recv[.]jsp

UNAVAILABLE (MD5: 145735911e9c8bafa4c9c1d7397199fc)

- FINEART loader
- Timestamp: 1996-09-08T20:44:37Z
- Loads MD5 af37b1453d318666af230d9335edd0c9

UNAVAILABLE (MD5: af37b1453d318666af230d9335edd0c9)

- HIDDENGIFT backdoor
- Timestamp: 2020-07-20T02:12:28Z
- C&C servers:
  - hxxp://www[.]allamwith[.]com/home/mobile/list[.]php
  - hxxp://www[.]conkorea[.]com/cshop/banner/list[.]php

UNAVAILABLE (MD5: df1e7a42c92ecb01290d896dca4e5faa)

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

- FINEART loader
- Timestamp: 1996-10-13T21:59:17Z
- XOR key: &#6*$LvOAgHyZ)d
- Loads MD5 fb84a392601fc19aeb7f8ce11b3a4907

UNAVAILABLE (MD5: fb84a392601fc19aeb7f8ce11b3a4907)

- HIDDENGIFT backdoor
- Timestamp: 2020-11-24T20:18:03Z
- C&C servers:
  - hxxp://www[.]jinjinpig[.]co[.]kr/Anyboard/skin/board[.]php
  - hxxp://mail[.]namusoft[.]kr/jsp/user/eam/board[.]jsp

ComStore[.]exe (MD5: 0812ce08a75e5fc774a114436e88cd06)

- FINEART loader
- Timestamp: 1996-04-05T00:15:49Z
- XOR key: SrZu8!pD509*@7Y
- Loads MD5 3a72889649faa2e21a68be3be3232c6d

UNAVAILABLE (MD5: 3a72889649faa2e21a68be3be3232c6d)

- HIDDENGIFT backdoor
- Timestamp: 2020-12-11T16:07:02Z
- C&C servers:
  - hxxp://www[.]ddjm[.]co[.]kr/bbs/icon/skin/skin[.]php
  - hxxp://snum[.]or[.]kr/skin_img/skin[.]php

AlgStore[.]exe (MD5: 1bb267c96ec2925f6ae3716d831671cf)

- FINEART loader
- Timestamp: 1996-04-05T00:15:49Z
- XOR key: !zGYX*ei$%HrW9#
- Loads MD5 3a72889649faa2e21a68be3be3232c6d

AppStore[.]exe (MD5: 118cfa75e386ed45bec297f8865de671)

- FINEART loader
- Timestamp: 1996-10-16T22:48:21Z
- Loads MD5 4d30612a928faf7643b14bd85d8433cc

UNAVAILABLE (MD5: 4d30612a928faf7643b14bd85d8433cc)

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

- HIDDENGIFT backdoor
- Timestamp: 2020-12-03T07:55:05Z
- C&C servers:
  - hxxp://www[.]jinjinpig[.]co[.]kr/Anyboard/skin/board[.]php
  - hxxp://mail[.]namusoft[.]kr/jsp/user/eam/board[.]jsp

LOOKINGGLASS

Other FINEART loaders containing LOOKINGGLASS were identified.

ExeInfoPE[.]exe (MD5: bf4a822f04193b953689e277a9e1f4f1)

- FINEART loader
- Timestamp: 2024-06-09T08:22:13Z
- Time appended to file: Tue Jan 19 15:15:47 2021
- XOR key: &#6*$LvOAgHyZ)d
- Loads MD5 85e4b3a92ee42d70fc609ae846d3fafa

UNAVAILABLE (MD5: 85e4b3a92ee42d70fc609ae846d3fafa)

- LOOKINGGLASS backdoor
- Timestamp: 2021-01-11T05:57:28
- C&C server: 45[.]58[.]112[.]77

ExeInfoPE[.]exe (MD5: 67220baf2a415876bee2d43c11f6e9ad)

- FINEART loader
- Timestamp: 2024-06-09T08:22:13Z
- Time appended to file: Tue Jan 19 15:15:47 2021
- XOR key: &#6*$LvOAgHyZ)d
- Loads MD5 85e4b3a92ee42d70fc609ae846d3fafa

ExeInfoPE[.]exe (MD5: 33c2e887c3d337eeffbbd8745bfdfc8f)

- FINEART loader
- Timestamp: 2024-06-09T08:22:13Z
- Time appended to file: Tue Jan 19 15:15:47 2021
- XOR key: &#6*$LvOAgHyZ)d
- Loads MD5 85e4b3a92ee42d70fc609ae846d3fafa

ExeInfoPE[.]exe (MD5: 38917e8aa02b58b09401383115ab549e)

- FINEART loader
- Timestamp: 2024-06-09T08:22:13Z
- Time appended to file: Fri Jan 15 10:12:31 2021

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

- XOR key: &#6*$LvOAgHyZ)d
- Loads MD5 85e4b3a92ee42d70fc609ae846d3fafa

ExeInfoPE[.]exe (MD5: ef3a6978c7d454f9f6316f2d267f108d)

- FINEART loader
- Timestamp: 2024-06-09T08:22:13Z
- Time appended to file: Tue Jan 19 15:04:48 2021
- XOR key: &#6*$LvOAgHyZ)d
- Loads MD5 85e4b3a92ee42d70fc609ae846d3fafa

3817608083 (MD5: 91038ff04bf85c19e377aef3381e47f9)

- FINEART loader
- Timestamp: 2021-09-04T09:02:45Z
- Payload is formatted as
  - <4-Byte Length><16-byte XOR Key><Base64 XOR Encoded Data>
- XOR key: jNaAaW(WZSOd2J$
- Only the first 15 bytes of the key is used
- Loads MD5 693e3d88a67872ebc0268f1475bfcbf9

UNAVAILABLE (MD5: 693e3d88a67872ebc0268f1475bfcbf9)

- LOOKINGGLASS backdoor
- Timestamp: 2020-11-27T06:08:11Z
- C&C server: 86[.]106[.]131[.]104

UNAVAILABLE (MD5: c827d95429b644e918d53b24719dbe6e)

- FINEART loader
- Timestamp: 1999-12-24T12:25:25Z
- XOR key: 74mlTgu(Uq1f&BF
- Loads MD5 a35a8c64870b9a3fe45348b4f2a93e75

UNAVAILABLE (MD5: a35a8c64870b9a3fe45348b4f2a93e75)

- LOOKINGGLASS backdoor
- Timestamp: 2020-11-24T13:41:50Z
- C&C server: 185[.]208[.]158[.]204

UNAVAILABLE (MD5: abaeecd83a585ec0c5f1153199938e83)

- FINEART loader
- Timestamp: 2021-10-12T10:40:53Z

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

- Payload is formatted as
  - <4-Byte Length><16-Byte Key>0x00<XOR Encoded Data>
- XOR key: wNmHK3J92E^KE4y
- Loads MD5 525cc10803d9858fca5dc4010925ba68

UNAVAILABLE (MD5: 525cc10803d9858fca5dc4010925ba68)

- LOOKINGGLASS backdoor
- Timestamp: 2020-12-13T06:48:00Z
- C&C server: 185[.]208[.]158[.]208

UNAVAILABLE (MD5: fffad123bd6df76f94ffc9b384a067fc)

- FINEART loader
- Timestamp: 1997-04-29T03:08:37Z
- Time appended to file: Mon Apr 19 09:31:39 2021
- XOR key: wNmHK3J92E^KE4y
- Loads MD5 92e34e16ea05360adab1e66521b989c4

UNAVAILABLE (MD5: 92e34e16ea05360adab1e66521b989c4)

- LOOKINGGLASS backdoor
- Timestamp: 2020-11-24T13:34:06Z
- C&C server: 185[.]208[.]158[.]208

vmware-vmx-gui[.]exe (MD5: cb9e18e21226a89ce2c26c695a989e0d)

- FINEART loader
- Timestamp: 1998-10-24T01:53:57Z
- XOR key: wNmHK3J92E^KE4y
- Loads MD5 643c2ad6067051e3daf7d08b4adeaed4

UNAVAILABLE (MD5: 643c2ad6067051e3daf7d08b4adeaed4)

- LOOKINGGLASS backdoor
- Timestamp: 2020-11-28T18:11:42Z
- C&C server: 193[.]56[.]28[.]251

IEXPLORE[.]EXE (MD5: 62eae43a36cbc4ed935d8df007f5650b)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- Time appended to file: Tue Sep 22 16:12:54 2020
- Payload is formatted as

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

    - <4-Byte Length><16-Byte XOR Key><Base64 XOR Encoded Data>
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

UNAVAILABLE (MD5: 0edb25adab3af46f3d900767a3247607)

- LOOKINGGLASS backdoor
- Timestamp: 2020-08-27T01:53:32Z
- C&C server: 23[.]229[.]111[.]197

IEXPLORE[.]EXE (MD5: d1a99087fa3793fbc4d0adb26e87efce)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: 3b494133f1a673b2b04df4f4f996a25d)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: d63bb2c5cd4cfbe8fabf1640b569db6a)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- Time appended to file: Wed Sep 23 20:18:39 2020
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: fc3c31bbdbeee99aba5f7a735fac7a7e)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- Time appended to file: Wed Sep 23 16:36:27 2020
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: 569246a3325effa11cb8ff362428ab2c)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: 8b378eabcec13c3c925cc7ca4d191f5f)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- Time appended to file: Tue Sep 22 20:35:31 2020
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: eef723ff0b5c0b10d391955250f781b3)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- Time appended to file: Mon Sep 21 19:33:17 2020
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: 5b387a9130e9b9782ca4c225c8e641b3)

- FINEART loader
- Timestamp: 2000-07-07T04:48:52Z
- Time appended to file: Tue Sep 22 16:24:07 2020
- XOR key: 0AeEeeEjoXYEU*v
- Loads MD5 0edb25adab3af46f3d900767a3247607

IEXPLORE[.]EXE (MD5: 159ad2afcab80e83397388e495d215a5)

- FINEART loader
- Timestamp: 1995-08-15T05:52:53Z
- XOR key: TSx&k*LhBLPw4BE
- Loads MD5 7b81ea543bb57d2b6db1610d8b424e95

UNAVAILABLE (MD5: 7b81ea543bb57d2b6db1610d8b424e95)

- LOOKINGGLASS backdoor
- Timestamp: 2020-09-21T05:07:59Z
- C&C server: 23[.]229[.]111[.]197

UNAVAILABLE (MD5: 3bf9b83e00544ac383aaef795e3ded78)

- FINEART loader
- Timestamp: 2023-11-28T00:41:25Z

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

- Time appended to file: Mon Oct 19 09:39:41 2020
- Loads MD5 5c41cbf8a7620e10f158f6b70963d1cb

UNAVAILABLE (MD5: 5c41cbf8a7620e10f158f6b70963d1cb)

- LOOKINGGLASS backdoor
- Timestamp: 2020-10-18T02:13:24Z
- C&C server: 10[.]101[.]30[.]127

Another sample of SILVERFROG was identified targeting the aerospace and defense industry.

airbus_job_opportunity_confidential[.]doc (MD5: 4fb3bd661331b10fbd01e5f3e72f476c)

- Creation date: 2021-06-05 16:14:00
- Last modified date: 2021:06:10 07:18:00
- Drops SILVERFROG DriverCacheSH[.]exe

DriverCacheSH[.]exe (MD5: b7dbb3bef80d04e4b8981ab4011f4bfe)

- SILVERFROG
- Timestamp: 2021-06-06T01:03:23Z
- C&C server: hxxps://shopweblive[.]com/image_slider[.]png

DriverCacheSH[.]exe (MD5: 9e54e1a831824f2cca3bbc2d8c5db108)

- SILVERFROG
- Timestomp: 2021-06-06 01:03:22Z
- C&C server: hxxps://shopweblive[.]com/image_slider[.]png

YARA Rules

```
rule MTI_Hunt_APT_SHATTEREDGLASS_Strings {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
    description = "Detects strings found in SHATTEREDGLASS"
    md5 = "d96fcd2159643684f4573238f530d03b"
    date = "06/23/2021"
    version = "1"
  strings:
    $1 = "cmd[.]exe /C ping 1[.]1[.]1[.]1 -n 1 -w 3000 > Nul & Del /f" fullword wide
    $2 = "Getting Key from Server Failed." fullword
    $3 = "ID : %S" fullword
    $4 = "IV : " fullword
    $5 = "Key : " fullword
```

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

```
  condition:
    (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and all of them
}

rule MTI_Hunt_APT_SHATTEREDGLASS_Message_Strings {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects a ransomware message found in SHATTEREDGLASS"
    md5 = "d96fcd2159643684f4573238f530d03b"
    date = "06/23/2021"
    version = "1"
  strings:
    $1 = "What gurantees do we give to you?" fullword
    $2 = "You can send 2 your encrypted file from your PC with your ID and decrypt it for
free." fullword
    $3 = "You just need little bitcoin." fullword
  condition:
    (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and all of them
}

rule MTI_Hunt_APT_SHATTEREDGLASS_Encryption {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects an encryption routine found in SHATTEREDGLASS"
    md5 = "d96fcd2159643684f4573238f530d03b"
    date = "06/23/2021"
    version = "1"
strings:
    $a_file_encrypt = { 6A 00 68 80 00 00 00 6A 03 6A 00 6A 00 [0-24] 68 00 00 00 C0 5?
[0-8] FF 15 [4-36] 5? 5? FF 15 [4-24] 68 10 20 00 00 E8 [4-80] 68 00 20 00 00 5? 5? FF 15 }
    $a_file_encrypt_contd = { 6A 01 6A 00 F7 ?? 5? 5? FF 15 [4-40] 5? 5? 5? E8 [4-40] E8 [4]
83 C4 04 [0-8] 6A 00 5? FF B5 [4] 5? 5? FF 15 }
    $get_encryption_key_from_c2 = { FF 15 [4] 85 C0 7E ?? 03 ?? 83 ?? 17 7C ?? 83 ?? 17 75
?? 8B ?? B? [4] B? 13 00 00 00 8B ?? 3B ?? 75 ?? 83 ?? 04 83 ?? 04 83 ?? 04 }
    $part_of_encrypt_hardcoded_reg = { B4 1B 88 [2] 88 [2] 8A ?? 32 ?? 32 ?? 88 [2] 8A ??
32 ?? 8A ?? 02 ?? C0 ?? 07 F6 EC B4 1B }
  condition:
     (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and
(uint16(uint32(0x3C)+0x18) == 0x010B) and all of them and @a_file_encrypt[1] <
@a_file_encrypt_contd[1]
}

rule MTI_Hunt_APT_HIDDENGIFT_Reused_Uninstall_Script {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects an uninstall script found in at least HIDDENGIFT, HANGMAN, and
```

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

```
LOOKINGGLASS"
    md5 = "fb84a392601fc19aeb7f8ce11b3a4907"
    date = "06/24/2021"
    version = "2"
  strings:
    $uninstall = {
406563686F206F66660D0A3A4C310D0A64656C20222573222573202225732220676F746F
204C310D0A64656C20222573220D0A }
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and $uninstall
}

rule MTI_Hunt_APT_BLANKCANVAS_Strings {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects strings found in BLANKCANVAS"
    md5 = "f2132947d0668084620c7687342c7bb9"
    date = "06/21/2021"
    version = "1"
  strings:
    $str1 = "SOFTWARE\\Classes\\.tlb" wide ascii
    $str2 = "CurrentVersion\\Run" wide ascii
    $str3 = "Shell\\Open\\Command" wide ascii
    $str4 = "error!" wide ascii
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and all of ($str*)
 }

rule MTI_Hunt_APT_BLANKCANVAS_Routine {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects a routine found in BLANKCANVAS"
    md5 = "f2132947d0668084620c7687342c7bb9"
    date = "06/21/2021"
    version = "1"
  strings:
    $hex = { 03 01 00 00 [1-10] 00 [1-38] 3F 00 0F 00 [1-2] 00 [1-12] 01 00 00 80 [1-206]
01 [1-2] 00 [1-88] 04 01 00 00 [1-10] 00 [1-32] 00 [1-12] 00 [1-2] 07 00 00 00 [1-20] 3F 00
0F 00 [1-6] 00 [1-2] 00 [1-2] 00 [1-12] 01 00 00 80 [1-78] 01 [1-2] 00 [1-56] 04 01 00 00 [1-
10] 00 [1-20] 00 [1-12] 00 [1-2] 07 00 00 00 [1-20] 3F 00 0F 00 [1-6] 00 [1-2] 00 [1-2] 00
[1-12] 01 00 00 80 }
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and $hex
 }

rule MTI_Hunt_APT_LOOKINGGLASS_Symbols {
  meta:
```

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

```
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects an uninstall script found in at least HIDDENGIFT and HANGMAN"
    md5 = "5c41cbf8a7620e10f158f6b70963d1cb"
    date = "06/21/2021"
    version = "1"
  strings:
    $str1 = "AVModuleUpdate@@" wide ascii
    $str2 = "AVModuleShell@@" wide ascii
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and all of ($str*)
 }

rule MTI_Hunt_APT_FINEART_String {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects a string found in FINEART"
    md5 = "f4d46629ca15313b94992f3798718df7"
    date = "06/23/2021"
    version = "1"
  strings:
    $str = "js9$_wR$3" wide ascii
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and $str
}

rule MTI_Hunt_APT_PAINTBRUSH_Strings {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects strings found in PAINTBRUSH"
    md5 = "2968c20a07cfc97a167aa3dd54124cda"
    date = "06/21/2021"
    version = "1"
  strings:
    $msg1 = "%s:%d -> OPENED!" wide ascii
    $msg2 = "%s:%d -> CLOSED!" wide ascii
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and all of ($msg*)
 }

rule MTI_Hunt_APT_PAINTBRUSH_Routine {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects a routine found in PAINTBRUSH"
    md5 = "2968c20a07cfc97a167aa3dd54124cda"
    date = "06/21/2021"
```

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

```
    version = "1"
  strings:
    $hex = { 00 01 00 00 [1-148] 01 [1-8] 01 [1-18] 04 [1-16] 04 [1-16] 06 [1-94] 00 01 00
00 [1-80] 00 01 00 00 [1-88] 00 01 00 00 [1-88] 00 01 00 00 [1-24] 01  [1-194] FF [1-6] 0A
[1-28] FF [1-24] 02 02 00 00 [1-14] 00 01 00 00 [1-16] 00 [1-110] 00 01 00 00 [1-96] 00 [1-
144] 10 [1-162] E8 03 00 00  }
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and $hex
 }

rule MTI_Hunt_APT_ARTCURATOR_Strings {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
    description = "Detects strings found in ARTCURATOR"
    md5 = "c31e4e02aeeeae188f4404a8ad6d9f03"
    date = "06/21/2021"
    version = "1"
  strings:
    $str1 = "----Google Chrome Password----" wide ascii
    $str2 = "Mozila Firefox Password----" wide ascii
    $str3 = "Internet Explorer Password----" wide ascii
  condition:
    (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and all of ($str*)
 }
```

Snort Rules
Disclaimer: These rules are meant for hunting and have not been tested to run in a production environment.

```
alert tcp any any -> any any ( msg:"Possible SHATTEREDGLASS or LOOKINGGLASS
detected"; content:"HTTP 1."; depth:7; content:" /member[.]php "; distance:1; within:14;
fast_pattern; content:"SSL3.4"; within:6; content:!"fast_pattern"; content:!"|0d
0a|Referer:"; content:!"|0d 0a|Cookie:"; threshold:type limit,track by_src,count 1,seconds
3600; sid:99999999;)
```

Please rate this product by taking a short four question survey

First Version Publish Date
July 06, 2021 07:45:00 PM

Threat Intelligence Tags

Affected Industry

- Aerospace & Defense

Target Geography

- South Korea

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

Intended Effect

- Military Advantage
- Financial Theft

Motivation

- Financial or Economic
- Military/Security/Diplomatic

Source Geography

- North Korea

Tactics, Techniques And Procedures(TTPs)

- Malware Propagation and Deployment
- Malware Research and Development
- Social Engineering
- Ransomware

Malware Family

- FINEART
- HIDDENGIFT
- SILVERFROG
- SHATTEREDGLASS
- PAINTBRUSH
- LOOKINGGLASS

Technical Indicators & Warnings

IP:	185[.]208[.]158[.]204
Identifier:	Related
Network Type:	network
Domain:	www[.]conkorea[.]com
Identifier:	Related
Network Type:	network
Domain:	mail[.]neocyon[.]com
Identifier:	Related
Network Type:	network
Domain:	www[.]jinjinpig[.]co[.]kr
Identifier:	Attacker
Network Type:	network
Malware Family:	HIDDENGIFT

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

Domain:	www[.]allamwith[.]com
Identifier:	Related
Network Type:	network
Domain:	mail[.]sisnet[.]co[.]kr
Identifier:	Attacker
Network Type:	network
Malware Family:	HIDDENGIFT
Domain:	www[.]ddjm[.]co[.]kr
Identifier:	Related
Network Type:	network
Domain:	shopweblive[.]com
Identifier:	Related
Network Type:	network
IP:	45[.]58[.]112[.]77
Identifier:	Related
Network Type:	network
IP:	10[.]101[.]30[.]127
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]jinjinpig[.]co[.]kr/Anyboard/skin/board[.]php
Malware Family:	HIDDENGIFT
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://mail[.]sisnet[.]co[.]kr/jsp/user/sms/sms_recv[.]jsp
Malware Family:	HIDDENGIFT
IP:	86[.]106[.]131[.]104
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://mail[.]namusoft[.]kr/jsp/user/eam/board[.]jsp
Malware Family:	HIDDENGIFT

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

IP:	23[.]229[.]111[.]197
Identifier:	Related
Network Type:	network
IP:	193[.]56[.]28[.]251
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://mail[.]neocyon[.]com/jsp/user/sms/sms_recv[.]jsp
Malware Family:	HIDDENGIFT
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]ddjm[.]co[.]kr/bbs/icon/skin/skin[.]php
Malware Family:	HIDDENGIFT
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]allamwith[.]com/home/mobile/list[.]php
Malware Family:	HIDDENGIFT
Domain:	snum[.]or[.]kr
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]conkorea[.]com/cshop/banner/list[.]php
Malware Family:	HIDDENGIFT
Identifier:	Attacker
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://shopweblive[.]com/image_slider[.]png
Malware Family:	SILVERFROG
Domain:	mail[.]namusoft[.]kr

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

Identifier:	Attacker
Network Type:	network
Malware Family:	HIDDENGIFT
IP:	185[.]208[.]158[.]208
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://snum[.]or[.]kr/skin_img/skin[.]php
Malware Family:	HIDDENGIFT
SHA1:	9d7ac32d7dd352931bb62bc2d2a26decf21ca93c
File Name:	dump[.]bin
Identifier:	Attacker
File Size:	144384
SHA256:	464eaa82103f6f479e0d62dd48d2dab8ece300458136c03165d20915ee658067
Type:	application/x-dosexec
MD5:	0edb25adab3af46f3d900767a3247607
Malware Family:	LOOKINGGLASS
SHA1:	032678cd7f48a6f5a1516daf897d05953076a4ce
File Name:	bf4a822f04193b953689e277a9e1f4f1
Identifier:	Attacker
File Size:	312880
SHA256:	b0d6aee39e988196fdc821895a1f1aa63d1c032ea880c26a15c857068f34bfd9
Type:	application/x-dosexec
MD5:	bf4a822f04193b953689e277a9e1f4f1
Malware Family:	FINEART
SHA1:	5028fd6fcbd431ada4bbabdb32cf4f0412a328ec
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	f62adc678eaadc019277640e6695143a45336c2f91019f5d9308812db1d07285
Type:	application/x-dosexec
MD5:	3b494133f1a673b2b04df4f4f996a25d
Malware Family:	LOOKINGGLASS
SHA1:	b4584e696cf189ad0cac03135bad12d4d1d0e835
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	803328

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

SHA256:	053f992fcf717d74e3a8e5e461d2b8b4dcefc2032d66f6a99283242cb39735cf
Type:	application/x-dosexec
MD5:	f22a09b3f55b2fbb788174e9c7e03825
Malware Family:	FINEART
SHA1:	6a6f362e4d93bd7dc1342c0c6c329dfb46b92925
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	463262
SHA256:	da787cf1f4fd829dd4a7637bec392438b793c5f9c920560197545d20b58691af
Type:	application/x-dosexec
MD5:	fffad123bd6df76f94ffc9b384a067fc
Malware Family:	FINEART
SHA1:	0bced0f20ef12fbab59593dcd02e4c75d852b671
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	252416
SHA256:	ed11e94fd9aa3c7d4dd0b4345c106631fe52929c6e26a0daec2ed7d22e47ada0
Type:	application/x-dosexec
MD5:	525cc10803d9858fca5dc4010925ba68
Malware Family:	LOOKINGGLASS
SHA1:	fb51917fde7984628f5b96f72229511c7879abac
File Name:	drivercachesh[.]bin
Identifier:	Attacker
File Size:	109568
SHA256:	1690ce43530acf725f33aa30f715855d226d63276557d0e33fbcaf9b5ff9b84c
Type:	application/x-dosexec
MD5:	9e54e1a831824f2cca3bbc2d8c5db108
Malware Family:	SILVERFROG
SHA1:	30c94b910ba251bcc98df0d9ac201b48f8d1c534
File Name:	c3cecb6c82be49658ba01872e0f643b9
Identifier:	Related
File Size:	656384
SHA256:	08f3e555d2bd9b13a493be15184b5d3426293e745cc122ff703bd84d2f490793
Type:	application/x-dosexec
MD5:	c3cecb6c82be49658ba01872e0f643b9
SHA1:	f632336918ab18ba397a5dd2f956d58c58a5f6ab
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	147968
SHA256:	1177105e51fa02f9977bd435f9066123ace32b991ed54912ece8f3d4fbeeade4
Type:	application/x-dosexec
MD5:	4d30612a928faf7643b14bd85d8433cc

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

Malware Family:	HIDDENGIFT
SHA1:	82d6fafd0dc9b10c277015570d9bc33bca170d94
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	656237
SHA256:	382a209ce5745c85507b0bd80b87496ad92128e6870199d0c33d6ddedc542dd1
Type:	application/x-dosexec
MD5:	c827d95429b644e918d53b24719dbe6e
Malware Family:	FINEART
SHA1:	8a3cad10d3f3fa07be7752296b017b6a367082c0
File Name:	DriverCacheSH[.]exe
Identifier:	Attacker
File Size:	130048
SHA256:	3b33b0739107411b978c3cbafb312a44b7488bd7adabae3e7b02059240b6dc83
Type:	application/x-dosexec
MD5:	b7dbb3bef80d04e4b8981ab4011f4bfe
Malware Family:	SILVERFROG
SHA1:	0eb4e40416ce2c1df30a01bc54bb21b17370b966
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	375856
SHA256:	4d03a981bed15a3bd91f36972d7391b39791c582bb2959a9be154a74bd64db31
Type:	application/x-dosexec
MD5:	3bf9b83e00544ac383aaef795e3ded78
Malware Family:	FINEART
SHA1:	7e9cbd2fe29ade9c92f66305bf9159e97252740d
File Name:	643c2ad6067051e3daf7d08b4adeaed4
Identifier:	Attacker
File Size:	186368
SHA256:	23eff00dde0ee27dabad28c1f4ffb8b09e876f1e1a77c1e6fb735ab517d79b76
Type:	application/x-dosexec
MD5:	643c2ad6067051e3daf7d08b4adeaed4
Malware Family:	LOOKINGGLASS
SHA1:	45829dbdb3e8ac4bcfc5f1df50a9683ff1f910ec
File Name:	undefined
Identifier:	Attacker
File Size:	328192
SHA256:	025b637c12c209927ccaaf97dc699c9bbe1dbb0b5eb2a57e66da2fa3130e1b32
Type:	application/x-dosexec
MD5:	91038ff04bf85c19e377aef3381e47f9
Malware Family:	LOOKINGGLASS

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

SHA1:	226fe3317091d2f8c615b795ec1eeed69e530ec4
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	1892b72c053ab48edae8305ef449f2b5391921efea8b1d7c37d6d29f59edc92e
Type:	application/x-dosexec
MD5:	5b387a9130e9b9782ca4c225c8e641b3
Malware Family:	FINEART

SHA1:	57ebbccc02d69fcb99dbc04f77fe8fc25416c7b2
File Name:	3a72889649faa2e21a68be3be3232c6d
Identifier:	Attacker
File Size:	147968
SHA256:	63bae252d796bc9ac331fdc13744a72bd85d1065ef41a884dc11c6245ea933e2
Type:	application/x-dosexec
MD5:	3a72889649faa2e21a68be3be3232c6d
Malware Family:	HIDDENGIFT

SHA1:	d331ec05ed4de11aaf512710620e501a21efbe30
File Name:	af37b1453d318666af230d9335edd0c9
Identifier:	Attacker
File Size:	99328
SHA256:	49a13bf0aa53990771b7b7a7ab31d6805ed1b547e7d9f114e8e26a98f6fbee28
Type:	application/x-dosexec
MD5:	af37b1453d318666af230d9335edd0c9
Malware Family:	HIDDENGIFT

SHA1:	01e0ccc0abb31b624c024933361637779fd8f368
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	d0fa0bfef8b199a42f4f33145274576e5a7edeb5522fb342af41fdc16e9021e2
Type:	application/x-dosexec
MD5:	d63bb2c5cd4cfbe8fabf1640b569db6a
Malware Family:	FINEART

SHA1:	ec062c8c6e77808ee2b3573f91eede294d572509
File Name:	vmware-vmx-gui[.]exe
Identifier:	Attacker
File Size:	311296
SHA256:	f78cabf7a0e7ed3ef2d1c976c1486281f56a6503354b87219b466f2f7a0b65c4
Type:	application/x-dosexec
MD5:	cb9e18e21226a89ce2c26c695a989e0d
Malware Family:	FINEART

SHA1:	ff57e56c9ffeb0c66ef6e23edbd5124dfba96c59

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	0dc3f66f4af3250f56a32f8e1b9e772c514f74718358d19c195e3950d370ea01
Type:	application/x-dosexec
MD5:	d1a99087fa3793fbc4d0adb26e87efce
Malware Family:	FINEART

SHA1:	5bb9faff8ff2b79700529cea46bc24814ce3ab33
File Name:	undefined
Identifier:	Attacker
File Size:	478208
SHA256:	6310cd9f8b6ae1fdc1b55fe190026a119f7ea526cd3fc22a215bda51c9c28214
Type:	application/x-dosexec
MD5:	1bb267c96ec2925f6ae3716d831671cf
Malware Family:	FINEART

SHA1:	43ef1dd0097da941dbcf64f00a790d6aae3a82f4
File Name:	AppStore[.]exe
Identifier:	Attacker
File Size:	516802
SHA256:	ed5fbefd61a72ec9f8a5ebd7fa7bcd632ec55f04bdd4a4e24686edccb0268e05
Type:	application/x-dosexec
MD5:	118cfa75e386ed45bec297f8865de671
Malware Family:	FINEART

SHA1:	a01318a2ae2cd1cc83c4c8531f8e6c4f9e3306b3
File Name:	0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c[.]exe
Identifier:	Attacker
File Size:	274946
SHA256:	4da0ac4c3f47f69c992abb5d6e9803348bf9f3c6028a7214dcabec9a2e729b99
Type:	application/x-dosexec
MD5:	df1e7a42c92ecb01290d896dca4e5faa
Malware Family:	FINEART

SHA1:	5e0ecb4f8776d4273d3e35bab784fc2d5689c625
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	2f53109e01c431c1c1acec667adee07cf907cdc4d36429022f915654c9b7113b
Type:	application/x-dosexec
MD5:	fc3c31bbdbeee99aba5f7a735fac7a7e
Malware Family:	LOOKINGGLASS

SHA1:	00fe9a63074922c5f8d4b99af4d901dc1f476690

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

File Name:	85e4b3a92ee42d70fc609ae846d3fafa
Identifier:	Attacker
File Size:	186368
SHA256:	bbddcb280af742ce10842b18b9d7120632cc042a8fe42eed90fc4bc94f2d71ac
Type:	application/x-dosexec
MD5:	85e4b3a92ee42d70fc609ae846d3fafa
Malware Family:	LOOKINGGLASS
SHA1:	df694ff44fe7d43dcc1d7eedd33253839347bbeb
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	312880
SHA256:	d26987b705f537b10a11fb9913d0acc0218a0c0ae5f27e6f821d6d987b1cd4c7
Type:	application/x-dosexec
MD5:	33c2e887c3d337eeffbbd8745bfdfc8f
Malware Family:	LOOKINGGLASS
SHA1:	ab76f74f61428d15ab4e1dacc0824d1770c34689
File Name:	threatneedle/suspectedsimilarity/6e710f6f02fdde1e4adf06935a296fd8
Identifier:	Attacker
File Size:	186368
SHA256:	868a62feff8b46466e9d63b83135a7987bf6d332c13739aa11b747b3e2ad4bbf
Type:	application/x-dosexec
MD5:	6e710f6f02fdde1e4adf06935a296fd8
Malware Family:	LOOKINGGLASS
SHA1:	4bc32527b96ba5a0d37f6ad182974c2c8c97a4a7
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	e83f5e0a51845d7078a3aca8ca7a5b786e8bdf284efd3e08b3472dbf3e098930
Type:	application/x-dosexec
MD5:	8b378eabcec13c3c925cc7ca4d191f5f
Malware Family:	FINEART
SHA1:	b365bed712582b3792096ff389e1755ff99a1f7e
File Name:	UNAVAILABLE
Identifier:	Attacker
SHA256:	588cdbd3ee3594525eb62fa7bab148f6d7ab000737fc0c311a5588dc96794acc
Type:	application/x-dosexec
MD5:	fb84a392601fc19aeb7f8ce11b3a4907
Malware Family:	HIDDENGIFT
SHA1:	4bab20413ccd74d84800c3441c383c3966a3de3b
File Name:	UNAVAILABLE

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

Identifier:	Attacker
File Size:	186880
SHA256:	8b3c8046fa776b70821b7e50baa772a395d3d245c10bdaa4b6171e0c5ce3f717
Type:	application/x-dosexec
MD5:	7b81ea543bb57d2b6db1610d8b424e95
Malware Family:	LOOKINGGLASS
SHA1:	d0c8a7efa1d9e7b9b8a570075a0df16fe2f3c67e
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	241152
SHA256:	ab194f2bad37bffd32fae9833dafaa04c79c9e117d86aa46432eadef64a43ad6
Type:	application/x-dosexec
MD5:	145735911e9c8bafa4c9c1d7397199fc
Malware Family:	FINEART
SHA1:	8b7b75a848664802d4421b8d0b7d38f22cc95da9
File Name:	693e3d88a67872ebc0268f1475bfcbf9
Identifier:	Attacker
File Size:	165888
SHA256:	e89e9011e4d803c8501cec9068de870fea0780f6200184bd061cd7a44dbb1340
Type:	application/x-dosexec
MD5:	693e3d88a67872ebc0268f1475bfcbf9
Malware Family:	LOOKINGGLASS
SHA1:	5c5becc3c6ca2e9abe478587da092f170b3f5e49
File Name:	UNAVAILABLE
Identifier:	Related
File Size:	159232
SHA256:	563333621d94aa9da3016a0cf04b56400c77dba993d8645a91bedf305594169b
Type:	application/x-dosexec
MD5:	779e53e6a0e08805617479d1f4ac4cca
SHA1:	ca7c2f05f49e9208ddc252e44812c2bdbbedcb80
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	318976
SHA256:	69bac736f42e37302db7eca68b6fc138c3aa9a5c902c149e46cce8b42b172603
Type:	application/x-dosexec
MD5:	159ad2afcab80e83397388e495d215a5
Malware Family:	LOOKINGGLASS
SHA1:	ea7be0d7778b64628c349b1f601950642b5dff9e
File Name:	92e34e16ea05360adab1e66521b989c4
Identifier:	Attacker
File Size:	252928

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

SHA256:	fec82f2542d7f82e9fce3e16bfa4024f253adee7121973bd9d67a3c79441b83c
Type:	application/x-dosexec
MD5:	92e34e16ea05360adab1e66521b989c4
Malware Family:	LOOKINGGLASS
SHA1:	9a2ddb06c92ca6b39ebfed1bbd23d6749a09af5f
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	222720
SHA256:	c500c9b8d4754fd891382f4bb1cfcaaa3cd14b87c5eafcced04170bc53d1a226
Type:	application/x-dosexec
MD5:	9a570c53b1a811aba02b2b76cc65b5eb
Malware Family:	PAINTBRUSH
SHA1:	c85f661a53b9deab53100670200a5a0e745c134c
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	7d7dc8125a26d9515d90a66bfd20d609820197c879030cb932d39b1c2998e9d4
Type:	application/x-dosexec
MD5:	62eae43a36cbc4ed935d8df007f5650b
Malware Family:	FINEART
SHA1:	f72cfe9b09c196f62da6bdc99dca6266bfb1a065
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	312880
SHA256:	9137e886e414b12581852b96a1d90ee875053f16b79be57694df9f93f3ead506
Type:	application/x-dosexec
MD5:	ef3a6978c7d454f9f6316f2d267f108d
Malware Family:	FINEART
SHA1:	3d8bdbdc08b6cefc7a44c18fafe7e4032c3b68bf
File Name:	a35a8c64870b9a3fe45348b4f2a93e75
Identifier:	Attacker
File Size:	252928
SHA256:	29c6044d65af0073424ccc01abcb8411cbdc52720cac957a3012773c4380bab3
Type:	application/x-dosexec
MD5:	a35a8c64870b9a3fe45348b4f2a93e75
Malware Family:	LOOKINGGLASS
SHA1:	995462ce4a1d8c10a81727de0a6b97426fe512f9
File Name:	f2132947d0668084620c7687342c7bb9
Identifier:	Related
File Size:	53760

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

SHA256:	61c9c8f595d0e5a7b11ff05797a1f947ba8a7b6d8afbfe5719be37d59be36afb
Type:	application/x-dosexec
MD5:	f2132947d0668084620c7687342c7bb9
SHA1:	35a4287e9688a83bf22aa5af35e2b35f9e9e84a6
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	87f389d8f3a63f0879aa9d9dfbbd2b2c9cf678b871b704a01b39e1eaa234020c
Type:	application/x-dosexec
MD5:	eef723ff0b5c0b10d391955250f781b3
Malware Family:	FINEART
SHA1:	c341002cc5f9214cc8fd71e633efef673267d1fd
File Name:	c341002cc5f9214cc8fd71e633efef673267d1fd
Identifier:	Attacker
File Size:	147968
SHA256:	5c2f339362d0cd8e5a8e3105c9c56971087bea2701ea3b7324771b0ea2c26c6c
Type:	application/x-dosexec
MD5:	fdc66cdabd46bc3b26aba4e59943726b
Malware Family:	HIDDENGIFT
SHA1:	7c8e2507b4149206ac9ad1d879b0d736b66991ba
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	186368
SHA256:	4aadf767491077ab83c6436cf108b014fc0bf8c3bd01cc6087a0f2b80564bc08
Type:	application/x-dosexec
MD5:	5c41cbf8a7620e10f158f6b70963d1cb
Malware Family:	LOOKINGGLASS
SHA1:	a2831445c73e6010e3ca50678fb5d49fbce13347
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	116224
SHA256:	ce534eb8de37b392b25546bfd1bb3c95c96ae6d14524a9241d2fffc02ae7b9c5
Type:	application/x-dosexec
MD5:	d96fcd2159643684f4573238f530d03b
Malware Family:	SHATTEREDGLASS
SHA1:	64b4c02d1d42b36bc87a7b5d92a287b1b3b15328
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	312880
SHA256:	f13aff9e1192c081c012f974b29bf60487385eed644d506d7f82b3538c2b035f
Type:	application/x-dosexec

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

MD5:	38917e8aa02b58b09401383115ab549e
Malware Family:	FINEART
SHA1:	d13f289c9dcc9aededdfcde7eabc75d35a240372
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	476672
SHA256:	b59e8f44822ad6bc3b4067bfdfd1ad286b8ba76c1a3faff82a3feb7bdf96b9c5
Type:	application/x-dosexec
MD5:	0812ce08a75e5fc774a114436e88cd06
Malware Family:	FINEART
SHA1:	704070f9a26cc6078f68d4dd48b9e7fef885c77b
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	762368
SHA256:	68e8f9f4f73f189c111c65fe1a9a591dff971bf0d2090d595a0a0c5af4308720
Type:	application/x-dosexec
MD5:	fb60f04f65d169a4471129e171d6b88d
Malware Family:	FINEART
SHA1:	faa5068d6129c5e6d2304f83fec63ed1e1901d0c
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	306224
SHA256:	ebe4befd2a7f941baa65248d5dea09de809e638ec8e8caffae322aa3b6863c1c
Type:	application/x-dosexec
MD5:	569246a3325effa11cb8ff362428ab2c
Malware Family:	FINEART
SHA1:	905f448dec32c96f5aa887a5085450f35381de5e
File Name:	airbus_job_opportunity_confidential[.]doc
Identifier:	Attacker
File Size:	931840
SHA256:	294acafed42c6a4f546486636b4859c074e53d74be049df99932804be048f42c
Type:	application/msword
MD5:	4fb3bd661331b10fbd01e5f3e72f476c
Malware Family:	SILVERFROG
SHA1:	f890ca1860cd53dda6d97ef7616baf26ef3686a7
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	581653
SHA256:	d231f3b6d6e4c56cb7f149cbc0178f7b80448c24f14dced5a864015512b0ba1f
Type:	application/x-dosexec
MD5:	abaeecd83a585ec0c5f1153199938e83
Malware Family:	LOOKINGGLASS

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

SHA1:	6b441c1f107ebad85e01b87dbbdbaa18ef2b41c5
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	312880
SHA256:	0e447797aa20bff416073281adb09b73c15433ab855b5cdb2d883f8c2af9c414
Type:	application/x-dosexec
MD5:	67220baf2a415876bee2d43c11f6e9ad
Malware Family:	FINEART

SHA1:	217470a07ecd399c45e3ab951ec70f8008b3abc3
File Name:	2968c20a07cfc97a167aa3dd54124cda
Identifier:	Attacker
File Size:	115713
SHA256:	7df30215533194a5003bbd3cb2dce23c524a6f8d4d20ae01d6b9ad32484c6d96
Type:	application/x-dosexec
MD5:	2968c20a07cfc97a167aa3dd54124cda
Malware Family:	PAINTBRUSH

SHA1:	727945fa45fd748f0ce03e0b8468e8fab3b05bc4
File Name:	f3fcb306cb93489f999e00a7ef63536b
Identifier:	Attacker
File Size:	476720
SHA256:	f4765f7b089d99b1cdcebf3ad7ba7e3e23ce411deab29b7afd782b23352e698f
Type:	application/x-dosexec
MD5:	f3fcb306cb93489f999e00a7ef63536b
Malware Family:	FINEART

SHA1:	6812be713e226fc15d575cc13e933e505324dd7c
File Name:	c31e4e02aeeeae188f4404a8ad6d9f03
Identifier:	Related
File Size:	702464
SHA256:	c4ef82749d415c5b05c4b435b029d56b949b0f244b82104429b6be184f84541f
Type:	application/x-dosexec
MD5:	c31e4e02aeeeae188f4404a8ad6d9f03

Version Information

Version:1.0, July 06, 2021 07:45:00 PM
New North Korean Malware Families Identified, Including Ransomware, Credential Harvester, and Others; Links to 'Andariel' Cluster

Confidential and Proprietary / Copyright © 2021 FireEye, Inc. All rights reserved.

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: https://intelligence.fireeye.com/reports/21-00014321

© 2021, FireEye, Inc. All rights reserved.