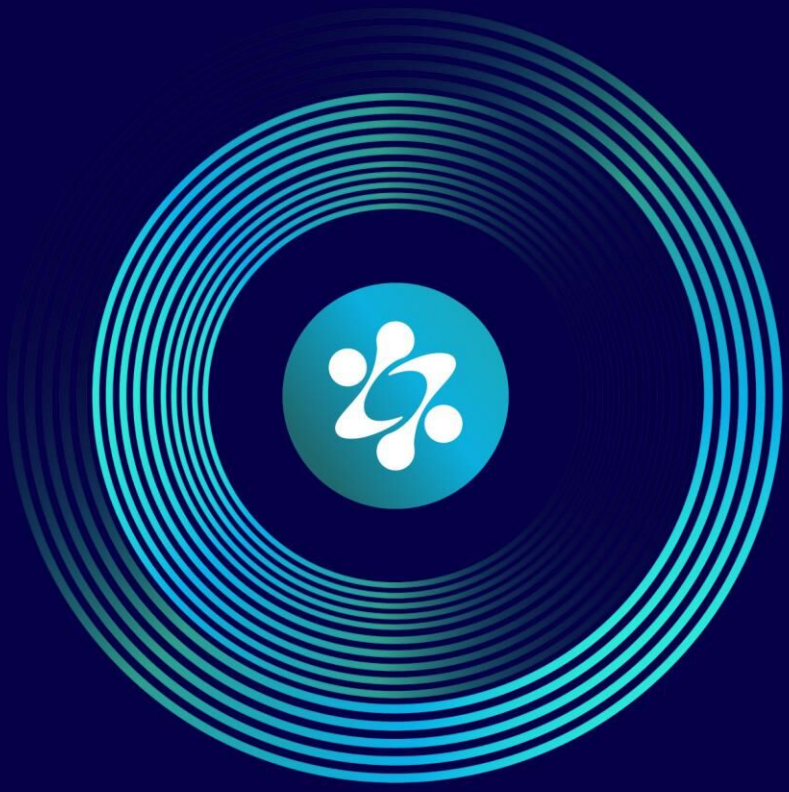

GhostLocker Ransomware Threat Intelligence Report

June 2024

INCD
Israel National
Cyber Directorate

Table of Contents

Executive Summary 3

Part I: Threat Intel Analysis 4

Variant Samples 5

Encryption Scheme 5

YARA Rule 5

Ransomware Incident TTPs 6

Part II: Indicators of Compromise 7

IPv4 Addresses 8

URL Paths 8

File Hashes 8

Tactics, Techniques, and Procedures 9

Executive Summary

The following report addresses the RaaS program initiated by GhostSec (A.K.A. GhostLocker) and later adopted by Stormous for continued operation. The information is based on OSINT resources and independent research by INCD. Although GhostSec advertised an info-stealer as well, this document will not be focusing on it and will solely detail findings regarding GhostLocker.

In the beginning of October (around October 6th), first posts from GhostSec's Telegram channel[1] came up indicating the development of a new RaaS program by the hacktivist group that was named "GhostLocker" with the prefix of the group's name. Later on, a post was published indicating the development of a new info-stealer tool, also supposedly made by the group and called "GhostStealer" – similarly to the naming of the RaaS program. In the most recent posts made by the group regarding their MaaS tools, they shared that they are working on what's called "GhostLocker REWRITE" – a revamped version of the aforementioned ransomware, that was released on January 2024 in another post.

On May 15th, GhostSec posted about their retirement from cyber-crime activities and returning to solely operate as hacktivists. They mentioned that they will move all management and operation of the RaaS program to the Stormous group which operate with GhostSec under the "Five Families" hacktivist super-group.

From the available information off of GhostLocker's postings and other OSINT resources, the INCD has dissected the known samples that indicate the ransomware is Python-based and compiled by Nuitka with code obfuscation, it targets Windows machines with AES encryption.

Several C2 servers are known to be used by GhostLocker, also featuring the affiliate login page. The ransomware communicates with the C2 using the mentioned IPs with specific paths that indicate progress and other commands.

See below research for further insights.

[1] Telegram channels associated with GhostSec and GhostLocker (t.me/GhostSecc; t.me/GhostLocker; @MonkeyCents; t.me/GhostSecSR)

Part I:

Threat Intel Analysis

INCD
Israel National
Cyber Directorate

Variant Samples

GhostLocker is a ransomware strain written in Python, compiled by an open-source project named Nuitka. The malware targets Windows devices, and encrypts files under a specific and configurable directory path. Once running the malware, Nuitka drops a .EXE file and multiple .PYD files in TEMP directory. The .EXE file contains the original malware's source code in Python, encoded in base64 for obfuscation. The following analysis is based on this observation.

Encryption Scheme

GhostLocker encrypts files using the Fernet library. It generates a key by calling Fernet.generate_key, which its underlying API calls to os.urandom (with 32-byte size buffer) and CryptGenRandom. As a result, the key length is 16 bytes and the rest of the buffer is used for a signature. Afterwards, GhostLocker initializes the Fernet class object with the mentioned above key as an argument, and calls the encrypt method. The encryption algorithm is AES-CBC, with a new random IV for each iteration. The encryption scheme is strong, and files affected cannot be decrypted without the encryption key.

YARA Rule

From the files surfaced by Uptycs' research a rule was compiled:

```
import "vt"
rule oct23_ghostsecraas_peexe{
    strings:
        $nuitka1 = "NUITKA_ONEFILE_PARENT" ascii fullword
        $hex1 = {31 35  0E  9F  44  49  4F}
    condition:
        uint16(0) == 0x5a4d and
        $nuitka1 and
        filesize < 10MB and
        filesize > 4MB and
        $hex1   and
        for any mutex in vt.behaviour.mutexes_created : (
            mutex == "WinSCPDragExtLogMutex" or
            mutex ==
"\\Sessions\\1\\BaseNamedObjects\\Global\\SyncRootManager"
    )
}
```

The YARA rule has surfaced 12 samples on VirusTotal Retro Hunt, some of them are already known from previous publications:

- 0e484560a909fc06b9987db73346efa0ca6750d523f2334913c23e061695f5cc
- 7e14d88f60fe80f8fa27076566fd77e51c7d04674973a564202b4a7cbfaf2778
- 65d3a922754af96d8d722859ac31f3de96522d50659c67607021f2ac728f9630
- 37fd38ff86b401b419c1ead45b93eb2410df16995cbc680533db1f5dbe072e41
- abcb441bcd754400997c9572260a610d54fe3c721307c29dc4af8216b9f14073
- abac31b5527803a89c941cf24280a9653cdee898a7a338424bd3e9b15d792972

- 11a706610985cc140e1ebd41300ec807044f99a99d010767b9baf5aad2812722
- 4844f44c9de364377f574e4d6a8a77dc0b4d6a67f21ccbf693ac366e52eaa8cb
- a725bae24208e89e53f891828ae34e27ca90b6ce2a5075317d8e742acc0f1c39
- 0b885bc615731fcf43da6896b226f5af906e6a0a083aa36ffd3d2cfd746e9ce9
- a8ae839e71c5d94177cdc3ed9fdd18cd2a34d660f7dadcb31df1e1dd0dce46d0
- ba0d8a9d01b0011042ab35c71457962cea2d43295c245be4c1454b6efc68bc18

Ransomware Incident TTPs

From one known incident where the address 195.2.79[.]117 was observed – it is known that two executable binaries were run that established connection with several IP addresses and domains. They are used to download files (some masquerading as documents) and disable security measures like Windows Firewall, manipulate logs and delete shadow copies.

A connection to a Google API's domain was made, probably to download further files and malware using the platform. Some of the connections established are known to be malicious and even used in other recent ransomware attacks; used as Cobalt Strike beacons; used for malware like browser hijackers and malware toolkits. Most IOCs probably relate to a botnet used in the attack.

The IP address 94.103.91[.]246, also known by one OSINT report to be related to GhostLocker's activity, was observed communicating with several endpoints on port 46466 in what appears to be a P2P communication (still not fully understood if that is part of the malicious activity and how). Most communications were in SMB/RDP/SQL ports (445/3306/1433/3389).

Part II:

Indicators of Compromise

INCD
Israel National
Cyber Directorate

IPv4 Addresses

88.218.61[.]141
88.218.62[.]219
195.2.79[.]117
94.103.91[.]246
41.216.183[.]31

URL Paths

/add
/incrementLaunch
/addInfection
/upload
/victimchat?id=[encryptionid
/login?next=
/incrementLaunches
/download
/incrementLaunch,Attackers
/addInfectioncrypto
/aes,Attackers
/addInfection,Attackers
/downloadp
/downloadastatus_codel
/addp
/incrementLaunchesT

File Hashes

MD5	SHA-1	SHA-256
c6208c4b168c2f8c433d6473e8ce3fb5	f9887e0cb144b3c68ff77017c6fef55f1da38b64	37214b37345bfbeeacf7b83ecb4e1ce0044acc2066d14e7ef9a87fd56a3b5975
69573601e8198a00481edee3e1c2267fc	b0ec5044e6b517d254283970f020825c021b855b	5bafabaf5913d6113566f74b8969c6f0250424ec48cd567c687f9db196fbcda5
91de74e4426f8c9118495c56d5fa6b2d	4797f529e20ff69179cab3dc21b81fbd3a62d6bd	7804e09b2ba224bae06bf23ca2a8b8d668d58b828a8d5aadbbb21c3b7e2acfc4
f001329114937fbc439f251c803ba825	95ae81de52655fac3f1b226f1896690566090640	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282eb24b7c55f
c30a14b595fa334084cd32fa60b3c827	3cd04b60b329388059cf58ce3ee6996559123cfa	c9f71fc4f385a4469438ef053e208065431b123e676c17b65d84b6c69ef6748a
8ad67a1b7a5f2428c93f7a13a398e39c	d4f71fc5479a02c8ff57c90fc67b948adb5604e0	8b758ccdfbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f443779e9
-	-	36760e9bbfaf5a28ec7f85d13c7e8078a4ee4e5168b672639e97037d66eb1d17
-	-	8fa28795e4cd95e6c78c4a1308ea80674102669f9980b2006599d82eff6237b3
-	-	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282eb24b7c55f
dfb5e2963e9bc48c904f4ac5978fe9ea	aa02aff8e6722e6e3733b8c884bc838360f08ccf	0e484560a909fc06b9987db73346efa0ca6750d523f2334913c23e061695f5cc

e6ec894f69899d14e3e8581939fe0685	35259aac75d64944fed5550aedc729f64762d497	4844f44c9de364377f574e4d6a8a77dc0b4d6a67f21ccbf693ac366e52eaa8cb
8506b32ea38dc3a844e72051750a75d9	396da9867520dc9077563ddfaf88e10fe9dfd6ea	65d3a922754af96d8d722859ac31f3de96522d50659c67607021f2ac728f9630
4119af0c5a12d6153e19514b4be993c4	a6e176a47659cc969836f0a24a976c8e876df992	15d874e24caf162bc58597ac5f22716694b5d43cf433bee6a78a0314280f2c80
bdc119efae38ea528c10adbd4c9000e4	57067dc15355c91fbbacf4f0f8b74555aae2dfd3	663ac2d887df18e6da97dd358ebd2bca55404fd4a1c8c1c51215834fc6d11b33
240632d05758d818be020342fd5d864b	0cb498c26a1e2d87da456956eb0e9bebce4f6ee5	a98f8468d70426ba255469a92d983d653f937d954e936e0ff5d9a0f44f1bdf70
dfbaa667c07fdd5ad2543ce98d097027	57b54340bb46950a708d0cb773101a77a9da0d95	ee227cd0ef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f
cd906ad0553a176d8737b4b85109687c	eb350ab1f913263011c710b1ede1805feb56d622	7d37eddf0b101ff2b633b2ffe33580bdb993a97fecc06874d7b5b07119b9ec99
81a136029d29d26920c0287faf778776	63ddf8364efe1130ecf788ab9ce566026a972cbe	7e14d88f60fe80f8fa27076566fd77e51c7d04674973a564202b4a7cbfaf2778
00c69252bc0e896e2a8b0a9a3d68e41e	37d01981b79ac2e397ef7264d6dcf568634c01c7	9b6be74c2c144f8bcb92c8350855d35c14bb7f2b727551c3dd5c8054c4136e3f
9c66d8fde4e6d395558182156e6fe298	e59372a29c43af4d15ed77784547aae34d3a6bdc	abac31b5527803a89c941cf24280a9653cdee898a7a338424bd3e9b15d792972
bea3d03f686c73622f08b1f0f8ec5b43	b24fde3aa3d2c42f99d14c43f0348fb43c6e50b7	4c09a012efff318b01a72199051815c5a7b920634fb6c76082673681f54f2ec3

Tactics, Techniques, and Procedures

Tactic	Technique
Impact	T1486 – Data Encrypted for Impact
Reconnaissance	T1592 – Gather Victim Host Information
Impact	T1489 – Service Stop T1490 – Inhibit System Recovery
Discovery	T1007 – System Service Discovery T1082 – System Information Discovery T1083 – File and Directory Discovery
Execution	T1059.003 – Command and Scripting Interpreter: Windows Command Shell T1059.006 – Command and Scripting Interpreter: Python
Defense Evasion	T1027 – Obfuscated Files or Information T1562.004 – Impair Defenses: Disable or Modify System Firewall
Command and Control	T1071.001 – Application Later Protocol: Web Protocols T1102 – Web Service