Lazarus Group's Mata Framework Leveraged To Deploy TFlower Ransomware

sygnia.co/mata-framework

Over the past few years, North Korea has turned its offensive cyber operations into a major source of income. On February 17, 2021, the US Department of Justice (DoJ) has indicted additional three North Korean (DPRK) military Reconnaissance General Bureau (RGB) personnel, with participating in a cyber-attacks that has allegedly included destructive cyber-attacks and the theft and extortion of over USD1.3bn.

The charges filed relate to Lazarus Group's (also known as Hidden Cobra) long-running cyber apparatus, financial theft and extortion, including multiple extortion schemes, WannaCry malware and the cyber-attack on Sony Pictures. A key technical component associated with Lazarus is the MATA malware framework, an advanced cross-platform malware framework, which was reported by Kaspersky on July 22, 2020, and by Netlab on December 19, 2019.

In a recent double extortion ransomware attack investigated by Sygnia, the threat actor leveraged a new and so far undocumented variant of MATA. This MATA variant was used by the threat actor to distribute and execute the TFlower ransomware.

When put together, the Netlab and Kaspersky publications along with the recent Sygnia findings, the new research indicates a connection or collaboration between the Lazarus Group and TFlower. While the nature of this collaboration is not yet clear and needs to be further validated, it may reflect the continues effort by North Korea to scale its cyber extortion business, as a major source for currency generation, including by collaborating with additional crime entities, creating such entities, "outsourcing" of capabilities, or selling of offensive tools to other groups.

This report details the connection between the North Korean MATA framework and TFlower, as well as the anatomy of the MATA backdoor and a wider threat research which revealed over 200 MATA malware framework C2 certificates leveraged since May of 2019 across over 150 IP addresses. The report also includes recommendation on detection and defending against MATA framework attacks.

THE KEY FINDINGS IN THIS REPORT ARE:

1. TFlower leverages or has ties to the MATA malware framework

The MATA backdoor was leveraged to deploy the TFlower ransomware. The threat group consistently referred to themselves as the "TFlower group".

2. The MATA malware framework is active and widespread

Since at least May of 2019, MATA operators have continuously utilized new servers, with over 150 IPs linked to the frameworks' C2. The analysis indicates that the group has possibly deployed over 150 command and control servers over time, with the latest one identified on February 4, 2021.

3. The threat actor is highly capable and implements systematic detection evasion techniques

Throughout the attack, the threat actor leveraged multiple tools including the MATA backdoor to systematically clear forensic evidence and attempt to evade detection by identifying and tampering with security products.

ANATOMY OF THE MATA BACKDOOR AND INFRASTRUCTURE

The Backdoor

The MATA backdoor consists of three file components: .EXE, .DLL and .DAT files, deployed in the "C:\Windows\System32" directory. All file names and hashes are unique per infected host indicating automatically generated polymorphic malware. The components are as follows:

1. Initial loader (EXE) — The malware is initially loaded by a .EXE file, which upon execution injects the .DLL loader component into an 'svchost.exe' process and modifies the LSA Security Package registry key to achieve persistence.

2. Loader (DLL) — The loader decrypts and executes the payload component stored in the .DAT file. It is loaded by 'lsass.exe' upon reboot to achieve persistence.

3. Payload (DAT) — The payload is an encrypted binary .DAT file which implements the backdoor functionality.

Once deployed, the backdoor provides the threat actor with remote code execution capability on infected machines via C2 servers. Additional functionality includes screen capture and network traffic tunneling.

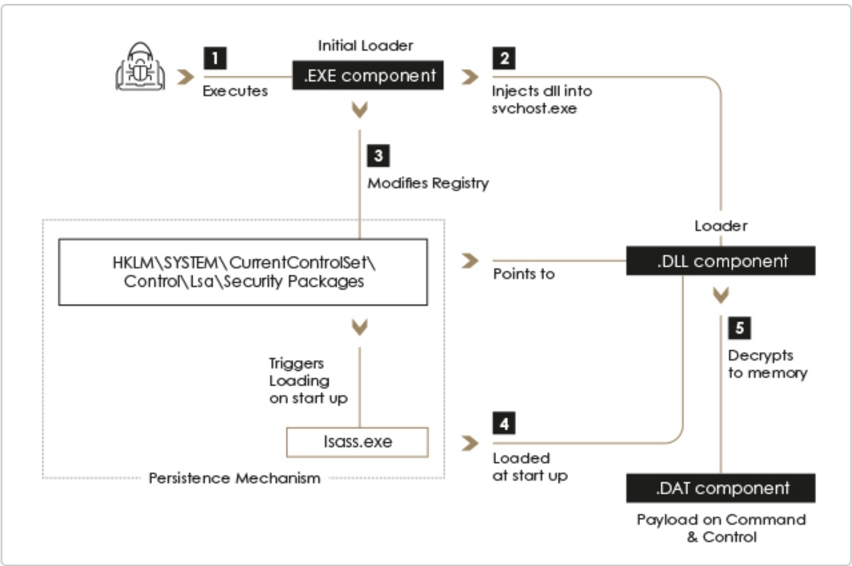
EXECUTION FLOW

The backdoor is deployed by executing the initial loader with the .DLL and .DAT file paths as arguments, injecting the .DLL file into 'svchost.exe' and loading the .DAT payload. The initial loader's file name consists of 5 alphabetic characters, randomly generated on each of the machines ('[A-Za-z]{5}\.exe').

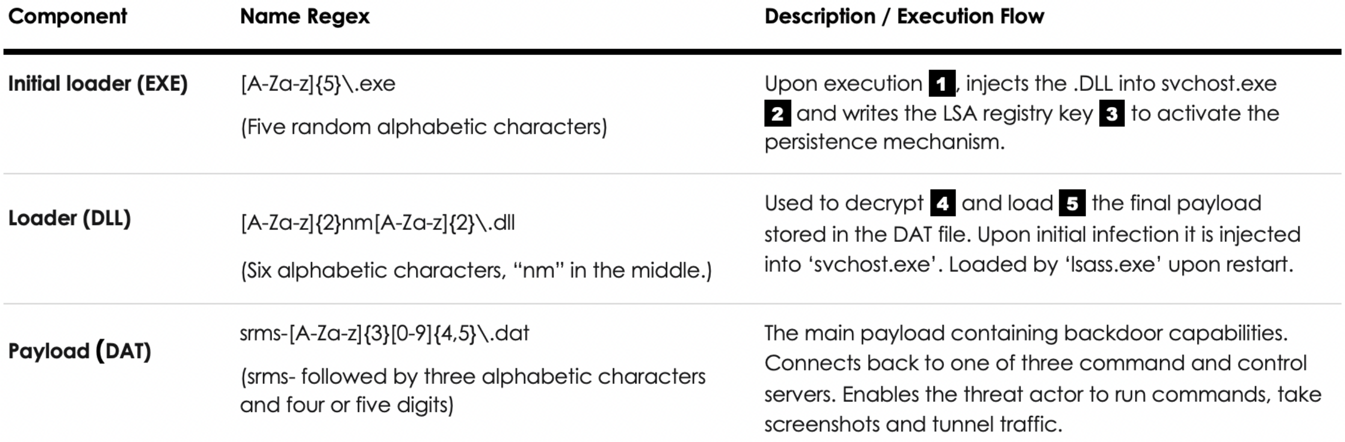
Upon execution, the initial loader modifies the following registry value in order to achieve persistency: "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages". The value modified is part of a Windows API called 'Security Support Provider' (SSP), which is used to extend the Windows authentication mechanism. After adding a .DLL stored in System32 to the 'Security Packages' value, 'lsass.exe' will automatically load the .DLL component on system startup or the next time the AddSecurityPackage Windows API function is called.

The file name of the .DLL consists of six alphabetic characters, the middle two being "nm" matching the following pattern: '[A-Za-z]{2}nm[A-Za-z]{2}\.dll'. Similar to the .EXE component, the name is unique on each of the infected machines. The .DLL itself implements limited functionality, and its main purpose is decrypting, loading and executing the final payload stored in the .DAT file.

The final payload stored in the .DAT file is a fully functional backdoor, establishing a command and control channel to the threat actors' servers. Similarly to the other components, its name was unique on each of the infected machines and followed a specific pattern: 'srms-[A-Za-z]{3}[0-9]{4,5}\.dat'.



Execution Flow: From initial execution to persistence mechanism.

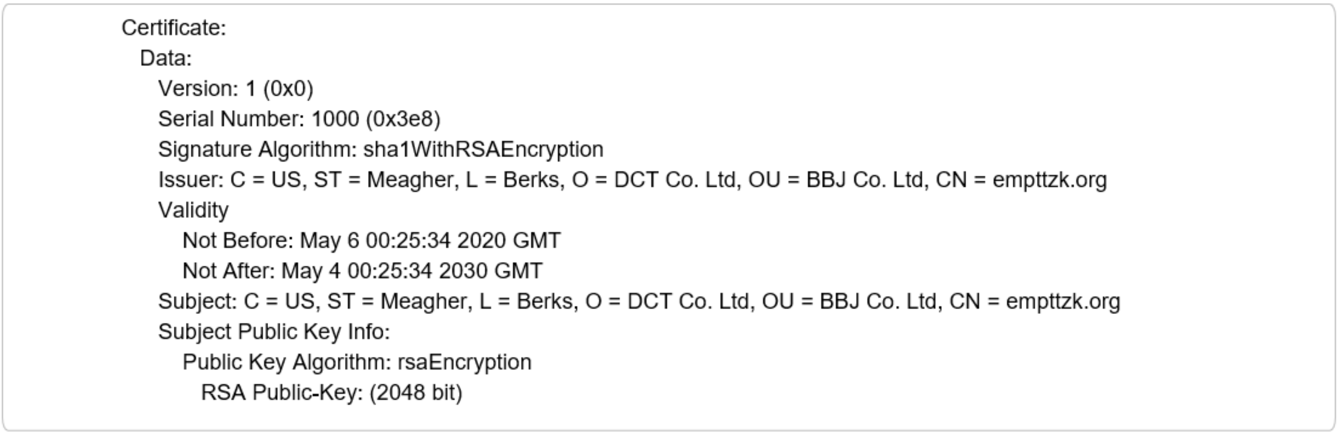


Component	Name Regex	Description / Execution Flow
Initial loader (EXE)	[A-Za-z]{5}\.exe (Five random alphabetic characters)	Upon execution 1, injects the .DLL into svchost.exe 2 and writes the LSA registry key 3 to activate the persistence mechanism.
Loader (DLL)	[A-Za-z]{2}nm[A-Za-z]{2}\.dll (Six alphabetic characters, "nm" in the middle.)	Used to decrypt 4 and load 5 the final payload stored in the DAT file. Upon initial infection it is injected into 'svchost.exe'. Loaded by 'lsass.exe' upon restart.
Payload (DAT)	srms-[A-Za-z]{3}[0-9]{4,5}\.dat (srms- followed by three alphabetic characters and four or five digits)	The main payload containing backdoor capabilities. Connects back to one of three command and control servers. Enables the threat actor to run commands, take screenshots and tunnel traffic.

COMMAND AND CONTROL INFRASTRUCTURE

Each of the samples identified by the Sygnia Incident Response team attempted to communicate to three command and control servers over SSL using port 443. The C2 servers were found in an encrypted binary configuration blob hardcoded into the .DAT payload. Each of the servers hosted a unique certificate, self-signed by the threat actor. Although the certificates on each of the servers were unique, they all shared similar technical features:

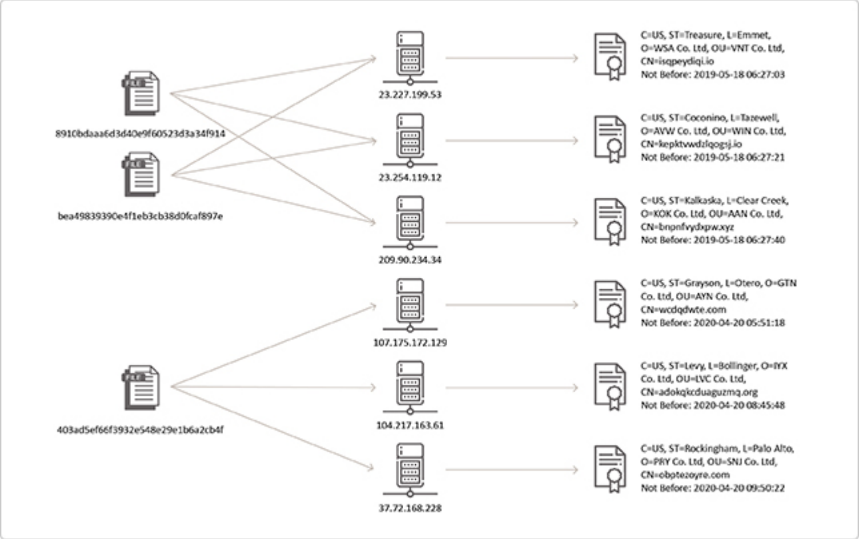
1. Randomly generated, long Common Name.
2. The usage of three capital letters followed by 'Co .Ltd' in the Organization (O) and Organization Unit (OU) fields of both issuer and subject.
3. Certificate serial number – 1000.
4. The “Validity: Not Before” timestamps of certificates tied to the same sample, are in close time proximity to one another. The “Validity: Not Before” timestamps represent the start of the certificate validity period.



```
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 1000 (0x3e8)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C = US, ST = Meagher, L = Berks, O = DCT Co. Ltd, OU = BBJ Co. Ltd, CN = empttzk.org
    Validity
      Not Before: May 6 00:25:34 2020 GMT
      Not After: May 4 00:25:34 2030 GMT
    Subject: C = US, ST = Meagher, L = Berks, O = DCT Co. Ltd, OU = BBJ Co. Ltd, CN = empttzk.org
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
```

Certificate Details: Example of malicious MATA C2 certificate.
The certificate “Validity: Not Before” timestamp is especially interesting, because the samples were first deployed in the network just several hours after the “Validity: Not Before” timestamp of their corresponding certificates. This could indicate that C2 servers are dynamically deployed for a specific operation, and the certificates are issued accordingly.

To further validate the ties between the MATA framework and the suspicious certificates, we attempted to tie other confirmed command and control servers to similar certificates. Out of 20 IPs found across 8 samples found in online repositories, 18 were confirmed to have historically hosted certificates with similar patterns.


8910bdaaa6d3d40e9f60523d3a34f914
bea49839390e4f1eb3cb38d0fcaf897e
403ad5ef66f3932e548e29e1b6a2cb4f
23.227.199.53
23.254.119.12
209.90.234.34
107.175.172.129
104.217.163.61
37.72.168.228
C=US, ST=Treasure, L=Emmet, O=WSA Co. Ltd, OU=VNT Co. Ltd, CN=isqpeydiqi.io Not Before: 2019-05-18 06:27:03
C=US, ST=Coconino, L=Tazewell, O=AVW Co. Ltd, OU=WIN Co. Ltd, CN=kepktvwdzlqogsj.io Not Before: 2019-05-18 06:27:21
C=US, ST=Kalkaska, L=Clear Creek, O=KOK Co. Ltd, OU=AAN Co. Ltd, CN=bnpnfvydxpw.xyz Not Before: 2019-05-18 06:27:40
C=US, ST=Grayson, L=Otero, O=GTN Co. Ltd, OU=AYN Co. Ltd, CN=wcdqdwte.com Not Before: 2020-04-20 05:51:18
C=US, ST=Levy, L=Bollinger, O=IYX Co. Ltd, OU=LVC Co. Ltd, CN=adokqkcduaguzmq.org Not Before: 2020-04-20 08:45:48
C=US, ST=Rockingham, L=Palo Alto, O=PRY Co. Ltd, OU=SNJ Co. Ltd, CN=obptezoyre.com Not Before: 2020-04-20 09:50:22

MATA Samples: Relations between MATA samples and the identified certificates.
Using the unique certificate patterns, Sygnia identified over 200 certificates and over 130 IP addresses affiliated with the MATA framework, starting as early as 2019.

Further analysis identified that as of June, 2020 the threat actor slightly modified the self-signed certificates pattern. Specifically, the following was changed:

1. Organization (O) and Organization Unit (OU) fields of both issuer and subject were changed to five random uppercase alphabetical characters instead of three.

2. Legitimate Common Name values such as ‘google.com’, ‘qq.com’ and ‘reddit.com’ were used instead of the random strings previously used.

At the time of publication, the latest certificates found were issued on February 4, 2021. The large number of certificates and C2 servers deployed over such a prolonged period of time suggests a well-resourced group with robust operational capabilities, likely attacking multiple targets simultaneously.

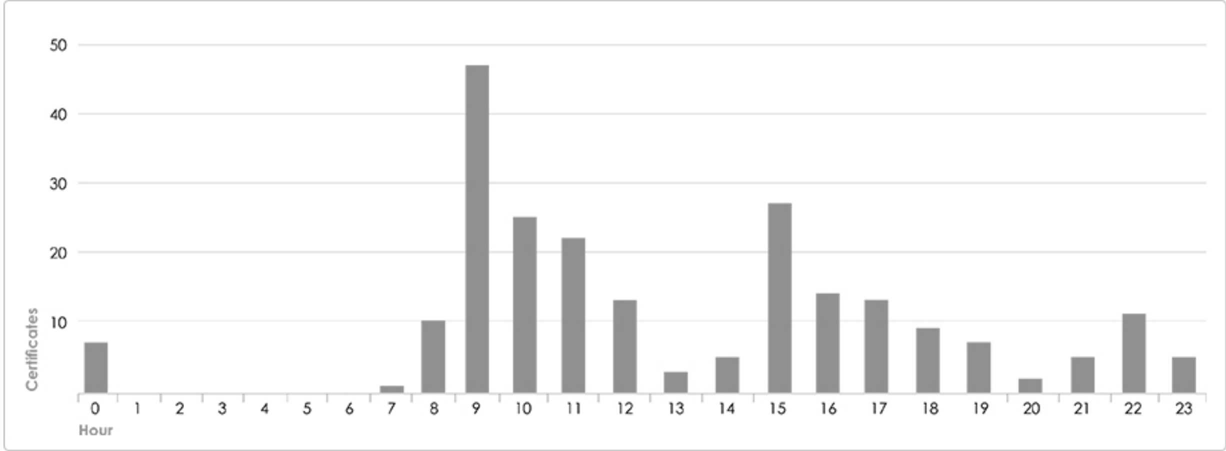
RELATION TO THE MATA MALWARE FRAMEWORK AND ATTRIBUTION

The backdoor and its infrastructure share significant attributes with the MATA malware framework:

- Over 95% of the functions in the .DLL loader component identified by Sygnia match functions in the MATA malware framework loader identified by Kaspersky, indicating they are closely related.
- The .DAT payload component identified by Sygnia writes its encrypted configuration to a registry key with a naming pattern of “HKLM\Software\Microsoft\[A-Za-z]{3}Net”. The orchestrator instances identified by Kaspersky save their configuration in a registry key with the same naming convention. The unencrypted configuration contains similar data to that mentioned in the Kaspersky report.
- The same SSL certificate pattern described above was also identified in SSL certificates served by 21 out of 31 MATA framework C2 IP addresses found within MATA framework malware samples reported by Netlab and Kaspersky.
- Certificates for IPs embedded in samples identified by Netlab and Kaspersky were issued within a short timeframe. This indicates the C2 servers for each of the samples were deployed together. The same behavior was observed in the samples identified by Sygnia.

Several other vendors, including Kaspersky and Netlab, linked the MATA framework to the Lazarus group, a threat actor affiliated with the North Korean government.

The MATA certificates “Validity: Not Before” timestamps are potentially indicative of the threat actor's work week, Monday to Saturday, as no certificates were issued on Sunday. Furthermore, no certificates were issued between 16:00 to 22:00 UTC, correlating with nighttime in UTC +9 or UTC +8 time zones. The vast majority of certificates were issued during working hours in the abovementioned time zones, suggesting the threat actor is most likely operating from East-Asia.



A histogram of certificates’ “Validity: Not Before” timestamps: showing the total number of certificates issued by hour in the day in a UTC+9 time zone.

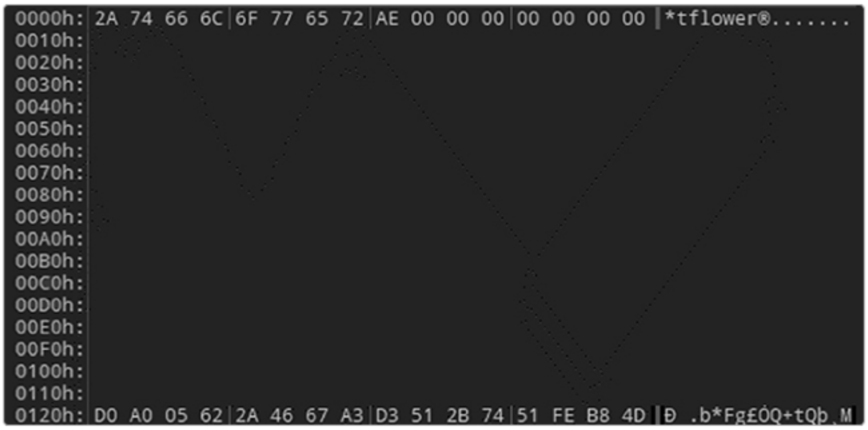
TFLOWER TIES TO THE MATA MALWARE FRAMEWORK

The TFlower ransomware campaign was covered by several technology news websites between September and November of 2019. However, since then very little information has been made public about the ransomware group or its operations.

In a recent TFlower ransomware case investigated by Sygnia, the threat actors had already removed all instances of the ransomware executable and it could not be recovered for reverse engineering. Nevertheless, forensic analysis performed identified several technical indications linking the encryption with the TFlower group with high certainty.

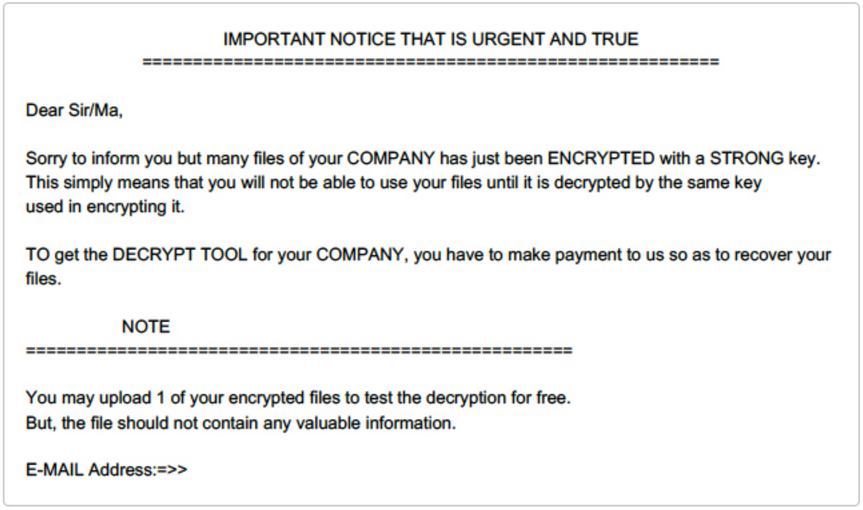
Analysis of the encrypted machines identified that the ransomware executable was deployed and executed using the MATA backdoor. Specifically, the path to the ransomware executable was found within the MATA backdoor memory space on encrypted machines. This raises the possibility that the Lazarus Group, which is largely affiliated with the North Korean government, is either the group behind TFlower or has some level of collaboration with it.

Alternatively, and although there are significant similarities to the TFlower ransomware, it is still possible that the threat actor was only masquerading as the TFlower group.



```
0000h: 2A 74 66 6C 6F 77 65 72 AE 00 00 00 00 00 00 00  *tflower®.......
0010h:
0020h:
0030h:
0040h:
0050h:
0060h:
0070h:
0080h:
0090h:
00A0h:
00B0h:
00C0h:
00D0h:
00E0h:
00F0h:
0100h:
0110h:
0120h: D0 A0 05 62 2A 46 67 A3 D3 51 2B 74 51 FE B8 4D  Ð .b*Fg£ÓQ+tQb M
```

The ransomware encrypted files throughout the filesystem, without appending any special file extension. The "*TFlower" string was prepended to the encrypted files.



IMPORTANT NOTICE THAT IS URGENT AND TRUE
===

Dear Sir/Ma,

Sorry to inform you but many files of your COMPANY has just been ENCRYPTED with a STRONG key.
This simply means that you will not be able to use your files until it is decrypted by the same key
used in encrypting it.

TO get the DECRYPT TOOL for your COMPANY, you have to make payment to us so as to recover your files.

NOTE
==

You may upload 1 of your encrypted files to test the decryption for free.
But, the file should not contain any valuable information.

E-MAIL Address:=>>

The ransom note left on the machines affected by the ransomware was named "!_Notice_!.txt". The ransom note itself is identical to ransom notes identified in previous TFlower attacks.

DEFENDING AGAINST MATA FRAMEWORK ATTACKS

The research into MATA framework operations was done primarily in the service of preventing future attacks. Our understanding of the threat actors behind these malicious operations reveals a large dynamic operation which can prove difficult to contain or easily detect.

The following are specific tactical recommendations which compliment more general security measures that can protect against these types of an attacks:

- Configure Process Protected Light (PPL) protection to prevent non-digitally signed LSA plugins to be loaded into the lsass.exe process.
- Proactively hunt for MATA malware framework IOCs and TTPs within the network, based on the MITRE ATT&CK breakdown and IOC provided below, with emphasis on the following:
- SSL traffic containing a self-signed certificate with the attributes described in the report.
- Outbound network communications towards the internet originating from the lsass.exe process
- Monitor for disabling of security products and log source tampering.

INDICATORS OF COMPROMISE

REGISTRY VALUES (REGULAR EXPRESSIONS)

- Registry Key: "HKLM\\Software\\Microsoft\\[A-Za-z]{3}Net"

- Registry Value Name: (default)
- Registry Value Type: "REG_BINARY"
- Registry Value Data: encrypted binary data

- Registry Key: "HKLM\\System\\CurrentControlSet\\control\\LSA"

- Registry Value Name: "Security Packages"
- Registry Value Type: "REG_MULTI_SZ"

- Registry Value Data: “[A-Za-z]{2}nm[A-Za-z]{2}”

FILE NAMES (REGULAR EXPRESSIONS)

- .EXE file component – “C:\\Windows\\System32\\[A-Za-z]{5}\.exe”

Highly susceptible to false positives

- .DLL file component – “C:\\Windows\\System32\\[A-Za-z]{2}nm[A-Za-z]{2}\.dll”

- .DAT file component – “C:\\Windows\\System32\\srms\-[A-Za-z]{3}\d+\.dat”

FILES REFERENCED IN THE REPORT (MD5)

- cef99063e85af8b065de0ffa9d26cb03
- 6de65fc57a4428ad7e262e980a7f6cc7
- 8910bdaaa6d3d40e9f60523d3a34f914
- bea49839390e4f1eb3cb38d0fcaf897e
- 80c0efb9e129f7f9b05a783df6959812
- 403ad5ef66f3932e548e29e1b6a2cb4f
- f05437d510287448325bac98a1378de1
- 22a968beda8a033eb31ae175b7e0a937

C2 SERVER CERTIFICATES

IP Address	Common Name	“Validity: Not Before” Timestamp	Organization	Org. Unit	Serial	SHA1
198.180.198.6	vurrsaw.io	2019-05-08T14:47:45Z	OVL Co. Ltd	IDQ Co. Ltd	1000	4fddb38848d0a3043d1
64.188.21.141	hnhxuapx.com	2019-05-08T15:02:01Z	WRK Co. Ltd	SVA Co. Ltd	1000	4e8c2bbdac96d4df655
96.44.130.126	hcsqwnya.com	2019-05-08T15:04:25Z	DKT Co. Ltd	MAO Co. Ltd	1000	64b628db142ee03dc9
173.44.48.241	qtwxcvh.net	2019-05-08T15:06:18Z	KIJ Co. Ltd	HVO Co. Ltd	1000	90a6731fcc1bf18eb47
103.63.2.209	uwmujaweipw.org	2019-05-08T15:13:25Z	NPP Co. Ltd	JKW Co. Ltd	1000	61ebfbf45dd7360811b
180.235.135.216	bkhboekbadgl.com	2019-05-08T15:15:22Z	FRK Co. Ltd	OET Co. Ltd	1000	91d4c3ed4336b4898b
104.143.37.87	ojpgynfdl.com	2019-05-08T15:17:38Z	QYZ Co. Ltd	TFJ Co. Ltd	1000	e9f88241ead0a454c54
103.63.2.211	uprdhgfk.org	2019-05-08T23:34:51Z	MFO Co. Ltd	RRJ Co. Ltd	1000	c1b5e79e754de08d68
103.63.2.184	zgvjwjuhvfwdcjme.xyz	2019-05-08T23:36:37Z	KMT Co. Ltd	MZX Co. Ltd	1000	78cb2ff0073f15c6f70f8
103.214.147.40	birtukgzz.io	2019-05-11T00:10:59Z	BMC Co. Ltd	EJV Co. Ltd	1000	9b3efb423d54fc96e8b
23.227.196.5	psldvwtsnzvfb.org	2019-05-11T00:12:03Z	ZID Co. Ltd	DAZ Co. Ltd	1000	b4042f03686336d1305
46.21.153.87	owxdawjfqueu.xyz	2019-05-11T00:12:27Z	RZF Co. Ltd	WSR Co. Ltd	1000	0a3c2caa5332916025
66.70.153.86	loerteademmexwga.xyz	2019-05-11T00:12:49Z	FHE Co. Ltd	III Co. Ltd	1000	ac9645de8cfc41c88bf3
23.227.199.53	isqpeydiqi.io	2019-05-18T06:27:03Z	WSA Co. Ltd	VNT Co. Ltd	1000	6ee218365ec9ff17eb0
23.254.119.12	kepktvwdzlqogsj.io	2019-05-18T06:27:21Z	AVW Co. Ltd	WIN Co. Ltd	1000	b138f782e23bc07d239

209.90.234.34	bnpnfvydxpw.xyz	2019-05-18T06:27:40Z	KOK Co. Ltd	AAN Co. Ltd	1000	e9321bdc979ae55a60
104.219.237.202	tpvccdrqlwft.io	2019-06-10T00:24:51Z	MGA Co. Ltd	BTH Co. Ltd	1000	8384997d8a807c34a1
107.172.57.13	nolrfot.net	2019-06-10T13:45:34Z	KTB Co. Ltd	IIS Co. Ltd	1000	fde0767ca94148a1bea
108.177.235.110	doywvaaqdhmtvm.io	2019-06-13T08:10:38Z	SCB Co. Ltd	KUA Co. Ltd	1000	7faf0d0f46ea2698b88d
23.95.67.143	cshveloxce.xyz	2019-07-01T03:09:46Z	BUR Co. Ltd	VGA Co. Ltd	1000	9f71d3a47cba2dacff5d
84.234.96.130	coejlawmj.net	2019-07-01T03:10:19Z	INK Co. Ltd	TRK Co. Ltd	1000	45f2465cc4d8157e41c
172.93.201.204	vflwshpmrha.com	2019-07-01T03:10:42Z	YWX Co. Ltd	MFA Co. Ltd	1000	7c1ce4cb7776cad2850
103.214.147.139	ogzphnvhgqfpqmlm.org	2019-07-02T00:22:01Z	JWA Co. Ltd	OHC Co. Ltd	1000	bfde0d8d8c1303b6cc6
64.188.19.117	gchcboujclol.xyz	2019-07-30T06:58:25Z	LHL Co. Ltd	YTF Co. Ltd	1000	fb2f3ffd2ac88dd62876
37.72.175.179	ojtkkwtzjggvz.xyz	2019-07-30T06:58:47Z	EJW Co. Ltd	RYT Co. Ltd	1000	471e268f24b938c8bda
23.81.246.179	gcjxswezjbdy.io	2019-07-30T07:02:19Z	XHQ Co. Ltd	OWZ Co. Ltd	1000	c39fa61ef4210f6726fb
149.255.35.15	jgybtvupucgvyjo.com	2019-07-31T06:22:39Z	RBJ Co. Ltd	PIL Co. Ltd	1000	eb847b373aa9284a22
104.143.37.55	ssmdtwssyz.xyz	2019-07-31T06:32:31Z	LVV Co. Ltd	ZQU Co. Ltd	1000	45f62d44f95a2b520b9
107.172.210.172	paodrrdwyyfj.org	2019-08-01T04:33:32Z	PVP Co. Ltd	QIR Co. Ltd	1000	66209d6585aa2ad80b
45.122.138.130	tejghhnxpbppafs.net	2019-08-06T07:45:16Z	CCO Co. Ltd	HFQ Co. Ltd	1000	ed96ea65fc7d34ed0a7
172.81.130.214	grlixnjkvtdtnvsc.io	2019-08-06T07:45:38Z	MYD Co. Ltd	XOR Co. Ltd	1000	15c96db7785d5e6866
104.143.37.54	izddauvlslqm.net	2019-08-07T08:00:13Z	AIZ Co. Ltd	QZA Co. Ltd	1000	a64b42eefc9b08ac06b
23.106.223.194	qgcrjrsxs.net	2019-08-07T08:15:14Z	GNL Co. Ltd	UPF Co. Ltd	1000	5360a98e4282da4206
167.114.56.231	mgrvnwtaqrzsdrv.org	2019-08-08T01:19:52Z	OVL Co. Ltd	GGJ Co. Ltd	1000	7c08dc40e773bc4b8c
107.172.83.139	ctrbxoxyh.io	2019-08-08T01:24:20Z	SDO Co. Ltd	CIB Co. Ltd	1000	0b189512af2b498fac0
216.45.54.11	mwqvqgquzknal.com	2019-08-08T01:24:47Z	SBY Co. Ltd	RET Co. Ltd	1000	1d5f886442d231b10fe
193.29.187.46	krcasfshnmwu.io	2019-08-09T13:44:14Z	FIY Co. Ltd	MRT Co. Ltd	1000	c7137530011eb2d0fca
104.227.244.140	gklkvcefc.xyz	2019-08-10T02:11:10Z	TIU Co. Ltd	CGP Co. Ltd	1000	d44c7ed99abd47db57
111.90.151.30	wuonxoqii.xyz	2019-08-10T02:24:38Z	HFQ Co. Ltd	BXJ Co. Ltd	1000	f84213fd940f019505e5
103.16.229.232	lymhmczmdsbxsryi.io	2019-08-23T13:20:06Z	XLP Co. Ltd	CTB Co. Ltd	1000	cad779915537cfed7c3
185.136.163.171	zaqxdbmudwzbl.xyz	2019-08-24T03:53:29Z	EYF Co. Ltd	UFF Co. Ltd	1000	5d0dc50f102bc9ced23

54.38.11.132	zcclzrwtysvclql.com	2019-08-26T02:27:33Z	CSJ Co. Ltd	WKN Co. Ltd	1000	55207654884899dece8
51.38.234.8, 103.16.229.233, 37.72.175.135	eavqdrkdt.net	2019-08-30T03:46:47Z	AYT Co. Ltd	DCI Co. Ltd	1000	caec7c0a802e4de75a6
23.227.199.21, 95.174.65.244	qwxniwspl.io	2019-09-03T00:56:01Z	PVP Co. Ltd	NEN Co. Ltd	1000	a4463133c2ec834d92f
23.227.196.116	kchinrxificfl.xyz	2019-09-20T09:31:27Z	BMB Co. Ltd	RLC Co. Ltd	1000	8730613623c457bb19f
74.121.190.121	qxyyyexemohemmil.com	2019-09-20T13:43:28Z	ZZC Co. Ltd	UOH Co. Ltd	1000	3ce1f8ace1a954a28d9
192.210.213.178	mevgtruvd.com	2019-09-20T13:47:08Z	EML Co. Ltd	PKM Co. Ltd	1000	febb999755a880203e8
69.61.74.29	nkirlyzy.io	2019-09-30T00:38:09Z	LLN Co. Ltd	LYG Co. Ltd	1000	d18ff190c769cf2bcf32a
172.93.189.77	yduyyoxu.io	2020-02-12T00:09:54Z	TJB Co. Ltd	BKQ Co. Ltd	1000	0d5cab6893e98032518
69.12.84.100	pqzajmdqhv.com	2020-02-19T11:04:18Z	HLR Co. Ltd	IVP Co. Ltd	1000	249d865fe438695d587
108.177.235.217	xvoomesesmxiysfs.io	2020-02-19T11:36:19Z	DWV Co. Ltd	LZW Co. Ltd	1000	19b6ad2fdf309c1090c7
104.168.62.33	ceagmjgpkkoohis.io	2020-02-19T12:46:59Z	DRU Co. Ltd	FUN Co. Ltd	1000	3e7fdd91198b48f0eae8
216.189.145.107	lzmaahdnkcy.net	2020-02-19T12:47:19Z	WGE Co. Ltd	UOH Co. Ltd	1000	399040a20e3891f1332
192.169.6.12	mxiiemkadyx.xyz	2020-02-19T12:48:00Z	ISQ Co. Ltd	LXK Co. Ltd	1000	4ffbc2b68bd9eaeb7d3f
104.219.237.210	ijlzzyuqtwvgzm.io	2020-02-19T12:57:15Z	MZN Co. Ltd	MDP Co. Ltd	1000	8660990c02e30933a64
149.255.35.25	zeyftccfvta.xyz	2020-02-20T02:10:13Z	GAK Co. Ltd	LWI Co. Ltd	1000	a7fcd5d5c2c57fd8a63f
172.93.184.62	cncvphssdmswy.io	2020-02-20T02:30:56Z	FTP Co. Ltd	UZX Co. Ltd	1000	88093735c7abdbeef29
23.227.199.69	hjnusrcxfsx.net	2020-02-20T02:37:14Z	DYH Co. Ltd	BGK Co. Ltd	1000	cae2fe70b7f98e4b3039
104.232.71.7	oaekzlcss.io	2020-02-20T02:59:24Z	MKT Co. Ltd	JJH Co. Ltd	1000	a151b18c72f9833e8ac
216.189.145.108	msutdedouhrvlipw.com	2020-02-20T05:46:46Z	HUY Co. Ltd	RQR Co. Ltd	1000	304261dcb04ce0fdd93
111.90.148.22	zxaqjnoq.com	2020-02-20T05:57:14Z	YRX Co. Ltd	KFT Co. Ltd	1000	14772f979839e3edab5
23.108.57.232	rbhllcdq.com	2020-02-20T07:10:56Z	INK Co. Ltd	MDW Co. Ltd	1000	c768b27d57e658efd6e
37.72.175.196	sonhmvsyqtj.com	2020-02-21T02:38:37Z	JPF Co. Ltd	RIO Co. Ltd	1000	6e55d351c22a077ce30
107.175.127.234	vtjmxqzyjdnfr.com	2020-02-21T02:39:04Z	EVQ Co. Ltd	KQA Co. Ltd	1000	8fdf10dd4f32dd546594
185.62.56.107	puqzedk.org	2020-02-24T01:00:54Z	HGJ Co. Ltd	RRB Co. Ltd	1000	b6aff0910dae32ccd833
172.93.220.108	mlntnbeikyak.io	2020-03-04T06:59:53Z	ZCO Co. Ltd	GNF Co. Ltd	1000	73e580ef0d8bcc4b910

209.127.18.108	kjjceey.com	2020-03-20T00:14:15Z	IHV Co. Ltd	DRU Co. Ltd	1000	76f753e777c8ed6ee3d
172.93.220.56	xvilcubqyxvpb.net	2020-03-20T00:28:03Z	GUW Co. Ltd	VSV Co. Ltd	1000	8901a2243f441855864
23.82.141.172	yfbfgjwuxj.xyz	2020-03-20T00:39:22Z	UKE Co. Ltd	DTE Co. Ltd	1000	acc8172dea21a5684f0
111.90.146.128	wswlmnrhscgj.com	2020-03-20T06:59:12Z	HKQ Co. Ltd	SCD Co. Ltd	1000	02c646ec8b88dcdc381
185.62.58.207	bvwaewachdyzpb.org	2020-03-20T23:48:59Z	VRZ Co. Ltd	JPO Co. Ltd	1000	e602553c2ac94f007af
67.43.239.146	uxusbtddbwgsz.org	2020-03-21T05:44:21Z	JLR Co. Ltd	ZHL Co. Ltd	1000	2cbbf4952add12302ca
104.143.36.33	zyfaywwrmxup.org	2020-03-23T00:11:04Z	GRE Co. Ltd	FLD Co. Ltd	1000	927eea1b33cfe8c0069
172.93.188.47	adehikjeb.net	2020-04-09T01:39:35Z	FVL Co. Ltd	RJS Co. Ltd	1000	e12c332b4f0e11b0de
185.62.56.106	blrewrclad.net	2020-04-09T08:23:39Z	FYV Co. Ltd	SCR Co. Ltd	1000	91e4a8f0176a0b2bd4f
67.43.239.181	duiywos.xyz	2020-04-09T08:32:31Z	HFD Co. Ltd	OGA Co. Ltd	1000	827b83175168959baa
103.214.147.39	rcvhlergjktdrh.io	2020-04-10T08:04:25Z	GNS Co. Ltd	CAO Co. Ltd	1000	128b37f254e92e2d91f
172.93.188.62	gqaoxbpozicjt.xyz	2020-04-11T00:05:22Z	TVH Co. Ltd	FNX Co. Ltd	1000	0547a8718765b8e833
107.175.172.129	wcdqdwte.com	2020-04-20T05:51:18Z	GTN Co. Ltd	AYN Co. Ltd	1000	8b41da1b919fafcbb60
104.217.163.61	adokqkcduaguzmq.org	2020-04-20T08:45:48Z	IYX Co. Ltd	LVC Co. Ltd	1000	99a79ad26ac0c9a96c
37.72.168.228	obptezoyre.com	2020-04-20T09:50:22Z	PRY Co. Ltd	SNJ Co. Ltd	1000	92c50351b2fa5982f2a
69.30.240.60	huqgniblte.com	2020-04-21T06:27:17Z	WIP Co. Ltd	EHG Co. Ltd	1000	74e2bc16b2eb69669ef
64.188.26.168	kudmgivpvuejmgog.io	2020-04-21T06:35:15Z	NBM Co. Ltd	UBE Co. Ltd	1000	f651db5f19216d2a036f
172.93.189.176	empttzk.org	2020-05-06T00:25:34Z	DCT Co. Ltd	BBJ Co. Ltd	1000	c001c42aba2d922ca04
185.62.56.47	nrkzktvgeoergf.net	2020-05-26T00:06:31Z	EXO Co. Ltd	HTD Co. Ltd	1000	7b66a217fcf61df2fe30
104.200.67.160	efqajqygqvo.io	2020-05-26T00:06:48Z	IRL Co. Ltd	YAZ Co. Ltd	1000	1290181d055156147e
103.214.147.138	pqvrtrikotcz.net	2020-05-26T00:38:29Z	SBG Co. Ltd	KJT Co. Ltd	1000	fe6615d6e40d45524ff3
96.9.210.193	jbqkxbwfqpmxf.net	2020-05-26T23:38:08Z	KRW Co. Ltd	GST Co. Ltd	1000	169584fe26f50c8b0f37
172.93.165.49	ykkywgzfjpf.io	2020-06-08T06:27:46Z	LIO Co. Ltd	VLP Co. Ltd	1000	19fd3b8a96452ba9a1c
107.172.30.141	mlgemilyaaxztct.net	2020-06-08T23:44:21Z	COF Co. Ltd	JUK Co. Ltd	1000	95038b25dcb22160a3
23.81.246.107	ffjdolvvxagjqn.com	2020-06-08T23:53:35Z	WNQ Co. Ltd	ZIZ Co. Ltd	1000	1899971acdc871d1161
172.87.222.6	znjpebeqb.org	2020-06-09T01:25:22Z	XAD Co. Ltd	UXJ Co. Ltd	1000	994bd84833827c1775

104.223.79.148	w3.org	2020-06-18T06:44:44Z	IMH Co. Ltd	YZQ Co. Ltd	1000	38fce40e0e6c028ac90
104.232.98.4	schema.org	2020-06-18T06:47:10Z	XPK Co. Ltd	OQO Co. Ltd	1000	2b3e68a625a88fffb50b
108.170.13.91	launchpadlibrarian.net	2020-06-18T06:47:42Z	SRR Co. Ltd	YWY Co. Ltd	1000	7993ab274ba47b8a31
192.111.149.132	google.com	2020-06-18T07:15:58Z	ZETIK Co. Ltd	JBXMI Co. Ltd	1000	8fab75e9930a614b80a
192.227.248.173	tmall.com	2020-06-18T07:17:02Z	BWJWM Co. Ltd	UMDGH Co. Ltd	1000	a3f893a132566f84d43
172.93.187.203	qq.com	2020-06-18T07:17:37Z	HSWMV Co. Ltd	AXWPM Co. Ltd	1000	486431e2d9024c44fde
23.82.141.50	baidu.com	2020-06-18T23:53:21Z	SQDLR Co. Ltd	SLZJO Co. Ltd	1000	e46da2ddb96d4d712f0
173.209.43.7	sohu.com	2020-06-19T00:17:43Z	OIBDB Co. Ltd	AUZIC Co. Ltd	1000	57bbceafe392c51480e
172.93.165.195	login.tmall.com	2020-06-19T03:30:12Z	RKVLG Co. Ltd	UYNCH Co. Ltd	1000	320dd14d32cba4ce25
104.232.98.18	a104.232.98.18.deploy.static.akamaitechnologies.com	2020-07-11T02:31:34Z	GTB Co. Ltd	UXQ Co. Ltd	1000	471756a047748e931e
149.255.35.19	a149.255.35.19.deploy.static.akamaitechnologies.com	2020-07-11T02:35:04Z	COM Co. Ltd	RPW Co. Ltd	1000	eb64df15cb2ca5e6fca
111.90.146.88	a111.90.146.88.deploy.static.akamaitechnologies.com	2020-07-11T02:38:27Z	IMN Co. Ltd	TSB Co. Ltd	1000	4d1a23a6d25dbb4d37
104.227.235.12	ubuntu.mirror.digitalpacific.com.au	2020-07-13T06:15:19Z	CEV Co. Ltd	HIE Co. Ltd	1000	3c822a64fdef9fd200dc
108.177.235.244	mirror.aarnet.edu.au	2020-07-13T06:16:44Z	HEJ Co. Ltd	CXD Co. Ltd	1000	83cfb13531f9a8a81ea
192.210.213.111	mirror.waia.asn.au	2020-07-13T06:18:31Z	LSA Co. Ltd	QTL Co. Ltd	1000	19a02f2453b15df76ec
63.141.234.106	live.com	2020-07-30T01:56:36Z	YQHXF Co. Ltd	RFMQT Co. Ltd	1000	b2ee5568161b0876ab
45.128.156.27	reddit.com	2020-07-30T01:57:33Z	AADTE Co. Ltd	OPGDQ Co. Ltd	1000	88773b940710b631a4
101.99.91.178	ubuntu.melbourneitmirror.net	2020-07-30T02:07:09Z	DFJ Co. Ltd	NYB Co. Ltd	1000	dbe39ba1d753f1a0a02
173.254.204.68	ubuntu.mirror.datamossa.io	2020-07-30T02:08:19Z	GQW Co. Ltd	GUI Co. Ltd	1000	9df88128e675307d274
111.90.138.218	netflix.com	2020-08-06T09:02:26Z	VFWBR Co. Ltd	RTXGR Co. Ltd	1000	03532ad6ed73f731f03
89.45.4.247	xinhuanet.com	2020-08-06T09:04:00Z	NUAXE Co. Ltd	JDOTY Co. Ltd	1000	519ad7e0cea23556b5
104.232.98.19	vk.com	2020-08-06T09:04:53Z	LCMBK Co. Ltd	AMJUR Co. Ltd	1000	9e984ad780434af4582
193.34.167.10	okezone.com	2020-08-06T10:24:30Z	RCVKL Co. Ltd	BWRNV Co. Ltd	1000	f2070d2c6aedc6ac0b5
107.173.28.8	csdn.net	2020-08-06T10:25:30Z	OKCOV Co. Ltd	JRVNW Co. Ltd	1000	06dbfb0ba7f155e40d7
204.12.225.21	myshopify.com	2020-08-06T10:26:26Z	OOWSC Co. Ltd	DTJHT Co. Ltd	1000	8c73fd5aa03b9259882
103.15.28.243	instagram.com	2020-08-10T14:31:12Z	HUTEV Co. Ltd	HSSYX Co. Ltd	1000	f60cb35c79241267f1e

64.188.26.168	mirror.intergrid.com.au	2020-08-17T07:14:05Z	LMT Co. Ltd	YEJ Co. Ltd	1000	412903b69697ad696b8
69.30.240.60	mirror.internode.on.net	2020-08-17T07:16:12Z	JEO Co. Ltd	XXL Co. Ltd	1000	fd4904bfd24de6da6be7
144.217.41.76	alipay.com	2020-08-17T08:44:46Z	JYRPP Co. Ltd	SESTG Co. Ltd	1000	eca6dbf704151283a21
103.16.229.232	mirror.launtel.net.au	2020-08-20T12:18:09Z	AYG Co. Ltd	ZYH Co. Ltd	1000	0e32a40bb83fec79614
107.152.213.117	mirror.netspace.net.au	2020-08-21T00:45:04Z	LDV Co. Ltd	YGO Co. Ltd	1000	19d8925e334d4116f4e
104.232.98.17	mirror.overthewire.com.au	2020-08-21T03:34:54Z	FAM Co. Ltd	EAW Co. Ltd	1000	1aab7a644e2de9b545e
172.93.178.108	mirror.realcompute.io	2020-08-21T03:36:10Z	GIF Co. Ltd	MVR Co. Ltd	1000	91cc94e09af78085095
172.87.222.3	yqeifkv.io	2020-08-31T06:51:03Z	TBD Co. Ltd	SBQ Co. Ltd	1000	cc2f66f648430deb60a1
23.94.139.92	yqpbbyoize.com	2020-08-31T06:51:58Z	VFQ Co. Ltd	URM Co. Ltd	1000	79d255f36da1ef71a366
172.241.27.117	bsdfjujierqeeog.org	2020-08-31T06:52:34Z	OLG Co. Ltd	IDP Co. Ltd	1000	b869ae4b3f11c9e7dd9
96.8.118.110	aliexpress.com	2020-09-07T06:24:17Z	CFCIU Co. Ltd	YRQEK Co. Ltd	1000	c5818365ccd628750e6
199.188.103.123	qnadslfndgo.com	2020-09-11T00:16:33Z	ASC Co. Ltd	UFJ Co. Ltd	1000	7e413302ef862b5c417
172.93.165.23	stackoverflow.com	2020-09-16T07:02:58Z	UIBGK Co. Ltd	MPNCO Co. Ltd	1000	700cd13b53c8bb66fd5
23.106.160.40	zhanqi.tv	2020-09-17T00:13:55Z	CZOWK Co. Ltd	NCQAQ Co. Ltd	1000	5fa1dd26de5449f41605
199.188.103.115	twitch.tv	2020-09-17T00:16:33Z	YZQVY Co. Ltd	NKNHX Co. Ltd	1000	9443af2bb8c281edc3d
67.43.239.213	panda.tv	2020-09-17T00:18:04Z	LRWUT Co. Ltd	UASTD Co. Ltd	1000	c67dca446f3dd6fb4336
149.56.200.203	force.com	2020-09-17T00:27:18Z	PFEOW Co. Ltd	RVAFN Co. Ltd	1000	bb53ba1e90f27896a6e
103.15.29.59	adjvwucfivllsv.org	2020-09-28T23:50:56Z	LWR Co. Ltd	FRN Co. Ltd	1000	8118c448070336884766
172.93.165.19	livejasmin.com	2020-09-29T00:18:03Z	YKLEC Co. Ltd	WZDSA Co. Ltd	1000	46eea848d03a4faed9e
103.214.147.209	chaturbate.com	2020-11-03T02:55:39Z	SIVDX Co. Ltd	EZDPF Co. Ltd	1000	22994c02534f74b442f6
54.39.204.190	adobe.com	2020-11-26T00:27:14Z	SGSPC Co. Ltd	OLBRG Co. Ltd	1000	8309da5cdafbaa578ea
101.99.91.247	apple.com	2020-11-26T00:28:28Z	DJNOC Co. Ltd	MVTDV Co. Ltd	1000	9083fab3637a60404bc
104.168.148.216	msn.com	2020-12-14T08:35:15Z	EMJYR Co. Ltd	ZJVKY Co. Ltd	1000	6656150ffdca1a739972
185.45.193.30	sogou.com	2020-12-14T09:52:49Z	NTTQF Co. Ltd	QUMVO Co. Ltd	1000	5cd0febfea57a9d4a846
172.93.165.155	wordpress.com	2020-12-17T10:29:45Z	AVGPZ Co. Ltd	BTEJQ Co. Ltd	1000	bbedc28ef631eef2d339
107.174.240.14	yy.com	2021-01-25T03:03:22Z	MZXEQ Co. Ltd	PCKPK Co. Ltd	1000	f9acf669ccf7a443d1df5

172.241.27.207	whatsapp.com	2021-01-25T06:55:17Z	TXJBZ Co. Ltd	VFHDF Co. Ltd	1000	2dce7f5ae09d1315ae0
67.219.150.3	medium.com	2021-01-26T01:31:50Z	OYZQK Co. Ltd	BWVOU Co. Ltd	1000	882ce7cd5405cafab60a
192.169.6.139	amazonaws.com	2021-01-26T03:07:12Z	ATDHB Co. Ltd	NXHQN Co. Ltd	1000	5ff8e100f48ed75cc0a8
74.222.26.164	imgur.com	2021-01-28T06:41:09Z	JCAFF Co. Ltd	QMOPZ Co. Ltd	1000	60852dcc1bbbd974154
193.34.167.183	bbc.com	2021-01-28T06:51:11Z	MQFPB Co. Ltd	WHPAW Co. Ltd	1000	a07d545c850c2897537
63.141.224.90	imdb.com	2021-01-28T08:07:54Z	HPCIS Co. Ltd	XUNQT Co. Ltd	1000	f18d9d4670b051c2645
3.239.189.175	ettoday.net	2021-01-28T08:08:54Z	ZYSOL Co. Ltd	JZQOD Co. Ltd	1000	d16a7642d2519fcd103
54.39.204.190, 23.94.37.55	cnn.com	2021-01-29T07:33:48Z	HTMSC Co. Ltd	XHIGN Co. Ltd	1000	e02961445c52cb9a2aa
144.168.224.235	freepik.com	2021-01-30T10:43:37Z	ZBGRS Co. Ltd	UCVED Co. Ltd	1000	875370a44ec1e53430b
194.15.112.193	spotify.com	2021-01-30T10:54:39Z	ORXOQ Co. Ltd	AFKIE Co. Ltd	1000	64cf462b1ff8cf77143ee
172.245.86.29	walmart.com	2021-01-30T10:55:40Z	NPTWC Co. Ltd	RZFVM Co. Ltd	1000	796068fe57f59d2d2532
107.174.20.79	etsy.com	2021-02-03T06:56:01Z	YEDHB Co. Ltd	VKQIE Co. Ltd	1000	c9ed6bcd81b64a9c925
23.227.202.105	ixlwyqfdrdcyift.com	2021-02-04T08:37:41Z	HDQ Co. Ltd	QFP Co. Ltd	1000	24c6b220ea7a2b5de58
104.243.143.78	jrwmngzk.net	2021-02-04T08:39:41Z	TJY Co. Ltd	TEZ Co. Ltd	1000	0a25f29bd5d6639057e

Showing 1 to 158 of 158 entries

MITRE ATT&CK BREAKDOWN

1. Persistence

- T1053.005 - Scheduled Task/Job: Scheduled Task
- T1547.005 - Boot or Logon Autostart Execution: Security Support Provider

2. Defense Evasion

- T1036.005 - Masquerading: Match Legitimate Name or Location
- T1055.001 - Process Injection: Dynamic-link Library Injection
- T1070.001 - Indicator Removal on Host: Clear Windows Event Logs
- T1070.003 - Indicator Removal on Host: Clear Command History
- T1070.004 - Indicator Removal on Host: File Deletion
- T1112 - Modify Registry
- T1562 - Impair Defenses

3. Credential Access

T1552.001 - Unsecured Credentials: Credentials in Files

4. Lateral Movement

- T1021.001 - Remote Services: Remote Desktop Protocol
- T1021.002 - Remote Services: SMB/Windows Admin Shares
- T1021.004 - Remote Services: SSH

5. Collection

T1113 - Screen Capture

6. Command and Control

- T1008 - Fallback Channels
- T1572 - Protocol Tunneling
- T1573.001 - Encrypted Channel: Symmetric Cryptography

7. Impact

T1486 - Data Encrypted for Impact

Contributors: Amitai Ben Shushan, Noam Lifshitz, Amnon Kushnir, Martin Korman and Boaz Wasserman.

Tag(s): Threat Report , Incident Response , Threat Research , Threat Hunting , Ransomware