A TrendLabs Report

Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors

Appendix

TrendLabs Security Intelligence Blog

Operation Iron Tiger is a targeted attack campaign discovered to have stolen trillions of data from defense contractors in the US, including stolen emails, intellectual property, strategic planning documents−data and records that could be used to destabilize an organization.

This document serves as an appendix for our research paper, "Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors." This appendix contains indicators of compromise and detection rules to detect some of the malware used by the threat actors during our investigation.

Malware Hashes and Detections

MD5	SHA1	Trend Micro Detection
785512dc380e303a37cd03b68a97c0ba	08afa64b23288c0414b379cb4e67c1a8dabea033	BKDR_MECA.A
0a40e22a4ffad11b7ec038acbb665d36	45ff712ae34512a9ac70060cec62a9b85f62804b	HKTL_ExPlug
c896320575d620e0f5333096dc726549	126a5972a0f6b0a5b0a2b52d7d848e8a9824f562	HKTL_IISExploit
941b83ff07e24e462275cb579cd3107e	9e61fb89551fa2640f30d00e322949d802355383	HKTL_HTRAN
ae4ac3399f0ee377ac4ccc8e92bf2338	f163b648ca1c134c7fefa9c6b1c9f24dc802e7f1	VBS_WIMXEC.A
ad48bbcfd7a1452de8b014fa5625ca3f	eeec12cb0dcc7c77a4ecee9facd2ccc1f3e2d93c	HKTL_DNSTUNNEL
7e843f735862a74ce74bef5bb5eac931	4df17c9e64f7277538141e384d4a372c60787f1a	TROJ_PLUGEX.C
e501dc14f1c1d3f7146c107dd7a77736	65b77d8b1ffd63a343c28e978487bc38b9792c6f	HKTL_PWDUMP
b254fe12263c68df7383e515d5afc6d6	d3fb95d0eeccd99c475c6b985a6c911bed69f50d	TROJ_PLUGEX.C
544642ffe59f54b9c5af4b20ec2678b2	3c6becafa9594601db64dc32c2c0384425a8fb5c	HKTL_PWDUMP
b9e8071bf83a5b1cf92892df85dc6295	bdf5d2565f855754442b45cb6b7af9a9c3504903	HKTL_PROXY
2d43058850eb6a2d36789fc105df1134	8c288818b39c7b738dd63c272893d0d24604ff62	TROJ64_WICRED.B
817ca5d90252eb49e143e903694b8856	0b68d3fd61b5d25f8aa5fb9d3b25428f33f55cf9	HKTL_PWDUMP
b47223ab622282cb5ae934cea8353a5b	d72ef43059ad0d5b4fc1e218e5257439ac006308	BKDR_GHOST.A

cf56cb65c4e5b4d7794147daeed0bf66	c3f5d5d52890fe72bd2fc4c08aaf538da73016d7	HTML_ASPSPY.A
c88e3c5818a88284c698eeb15f943f06	392cb13e762c65694b845472c77db15f61d0f8d8	HKTL_PWDUMP
9b72f87e92cd813432c7749d50809da9	4e3b1d957f5f4a568d5162638df94eb580ac6f77	HKTL_DOSEMU
9c6b38fb084075564caa5f881a5623d3	b27277142f4b4f71a757630a73014daae9ecfeb	HKTL_ASPXSPY
7458768d19b90b7911042d390c7a31f1	e7dfab16ac7989fef56f37de863647a53a32ecaa	HKTL_PWDUMP
1af84f059d511e2efb2e33527a99545a	8f36b41994719b1ad4a451d0aa387f7e67382230	VBS_WIMXEC.A
bdd98cb736322a80a31de2d027460470	856c3252fbc3d0e17d7d65cddff1ebbbab48496d	HKTL_IISEXPLOIT
2304a87e41f922bb03abc70fea11b491	c792029bcbd793433ba755396fe3b946dd352d97	HKTL_NBTSCAN
983eaa00360f85cf84e7d5954b9c3e70	add6f880705b4aaf4b22b60dd67ca9034694550d	HKTL_PORTCON
4dfaa46a80334af32f18dc1663b54537	ebf264ac75adbb82e28633865a9e453f3a0c8829	HKTL_PWDUMP
2c65085e7c71fa2c02c9b65e9b747e5b	afce5e56fc9bd1774d0cbbab1df205d0152fc632	HKTL_DNSTUNNEL
ad4a1e7c3728a61c2baeda77d607315d	ab68576e3cf6bf8020cf15a83390ebf9d545389b	HKTL_MIMIKATZ
f7146691adea573548fa040fb182f4fe	a346588c70751815bbb4c0922ea2c5e1ab9953db	HKTL_PORTCON
e5680224b064a5ee2d4094972291ba50	9484bb1b1c0e39355a66b20fc361846ce1f063e0	HKTL_HTRAN
858eaa588a5e30cd5156b27f72caa0fe	8c8f12ae866c38931e19d67fadc19bd18aaf0865	BKDR_GHOST.EJPZ
f7b106acc281a9aa395fb944c858c0c0	7b34f24703b5415bc46fdab3801ac79e3e82242a	BKDR_GHOST.EJPZ
37eec1a29d316ed1e5e766b599dc32a1	75f098d6b3f217aba4c068b12896c332216fc6b3	BKDR_PLUGX.XXT
edcd6d338aa7513c31f30ecb17fb4e70	50d2fef4e680072441084053773350d9ba60cac6	TROJ_DLODR.POLJ
49378c17c1a6fc653878a702b2cf7147	4883376735f981386e473318482fadfe90edc670	HKTL_MIMIKATZ
5bb03ecf2cc223d5254b6196c1654339	3ea58b2ff30ee1053a4053c681042516cb57038e	HKTL_PROXY
2db49bc54d596e38919092bebfaf8520	3d3db9d8da0eba33444c73b6f85a4fd98a685055	HKTL_MIMIKATZ
2a09b043a267b9a42b696fe2396749d9	14a4b7cd0215a3d512f97d6ec4072a784f123527	HKTL_MIMIKATZ
a173106fa27ac9861054dbf881ba568a	396af3ae018a9e251a832cce8aae1bcaa11cdc05	BKDR_GHOST.EJQA
9168ee3fe4f788d576cc6d438f226bae	0ad2796b1312af4db975a3978ede19e939e42846	HKTL_HTRan

78db8a38729861b3eaa8acc509a24a76	54649413507ee3bf242f541e3fc87bae6c033dfe	TROJ_PLUGEX.B
7e456d1136c832357909647a9ec66e2b	cf3d4646481b331a697dd15cc5587286f3b99dda	HKTL_PWDUMP

Fraudulent domains/IP addresses

- mac.pm
- d99net.net
- gameofthrones.ddns.net
- user.qzone.qq.com/1479457083
- ys168.com
- *.shangxian.info
- *.mail1.info
- xssok.blogspot.com
- phpxss.lofter.com
- exenull1.appspot.com
- chrome.servehttp.com
- update.gtalklite.com

YARA Rules

Rule IronTiger_ASPXSpy

```
rule IronTiger_ASPXSpy
{
meta:
	author="Cyber Safety Solutions, Trend Micro"
	comment="ASPXSpy detection. It might be used by other fraudsters"
strings:
        $str1="ASPXSpy" nocase wide ascii
        $str2="IIS Spy" nocase wide ascii
        $str3="protected void DGCoW(object sender,EventArgs e)" nocase wide ascii

condition:
        any of ($str*)
}
```

Rule IronTiger_ChangePort_Toolkit_driversinstall

```
rule IronTiger_ChangePort_Toolkit_driversinstall
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"

                $str1="openmydoor" nocase wide ascii
                $str2="Install service error" nocase wide ascii
                $str3="start remove service" nocase wide ascii
                $str4="NdisVersion" nocase wide ascii

        condition:
                $mz at 0 and (2 of ($str*))
}
```

Rule IronTiger_ChangePort_Toolkit_ChangePortExe

```
rule IronTiger_ChangePort_Toolkit_ChangePortExe
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"

                $str1="Unable to alloc the adapter!" nocase wide ascii
                $str2="Wait for master fuck" nocase wide ascii
                $str3="xx.exe <HOST> <PORT>" nocase wide ascii
                $str4="chkroot2007" nocase wide ascii
                $str5="Door is bind on %s" nocase wide ascii

        condition:
                $mz at 0 and (2 of ($str*))
}
```

Rule IronTiger_dllshellexc2010

```
rule IronTiger_dllshellexc2010
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"
                comment="dllshellexc2010 Exchange backdoor + remote shell"

        strings:
                $mz="MZ"

                $str1="Microsoft.Exchange.Clients.Auth.dll" nocase ascii wide
                $str2="Dllshellexc2010" nocase wide ascii
                $str3="Users\\ljw\\Documents" nocase wide ascii

                $bla1="please input path" nocase wide ascii
                $bla2="auth.owa" nocase wide ascii

        condition:
                ($mz at 0) and ((any of ($str*)) or (all of ($bla*)))
}
```

Rule IronTiger_dnstunnel

```
rule IronTiger_dnstunnel
{
meta:
        author="Cyber Safety Solutions, Trend Micro"
        comment="This rule detects a dns tunnel tool used in Operation Iron Tiger"

strings:
        $mz="MZ"
        $str1="\\DnsTunClient\\" nocase wide ascii
        $str2="\\t-DNSTunnel\\" nocase wide ascii
        $str3="xssok.blogspot" nocase wide ascii
        $str4="dnstunclient" nocase wide ascii

        $mistake1="because of error, can not analysis" nocase wide ascii
        $mistake2="can not deal witn the error" nocase wide ascii
        $mistake3="the other retun one RST" nocase wide ascii
        $mistake4="Coversation produce one error" nocase wide ascii
        $mistake5="Program try to use the have deleted the buffer" nocase wide ascii

condition:
        ($mz at 0) and ((any of ($str*)) or (any of ($mistake*)))
}
```

Rule IronTiger_EFH3_encoder

```
rule IronTiger_EFH3_encoder
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"

                $str1="EFH3 [HEX] [SRCFILE] [DSTFILE]" nocase wide ascii
                $str2="123.EXE 123.EFH" nocase wide ascii
                $str3="ENCODER: b[i]:=" nocase wide ascii

        condition:
                $mz at 0 and (any of ($str*))
}
```

Rule IronTiger_GetPassword_x64

```
rule IronTiger_GetPassword_x64
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"
```

```
	strings:
		$mz="MZ"

		$str1="(LUID ERROR)" nocase wide ascii
		$str2="Users\\K8team\\Desktop\\GetPassword" nocase wide ascii
		$str3="Debug x64\\GetPassword.pdb" nocase wide ascii

		$bla1="Authentication Package:" nocase wide ascii
		$bla2="Authentication Domain:" nocase wide ascii
		$bla3="* Password:" nocase wide ascii
		$bla4="Primary User:" nocase wide ascii

	condition:
		$mz at 0 and ((any of ($str*)) or (all of ($bla*)))
}
```

Rule IronTiger_GetUserInfo

```
rule IronTiger_GetUserInfo
{
	meta:
		author="Cyber Safety Solutions, Trend Micro"

	strings:
		$mz="MZ"

		$str1="getuserinfo username" nocase wide ascii
		$str2="joe@joeware.net" nocase wide ascii
		$str3="If . specified for userid," nocase wide ascii

	condition:
		$mz at 0 and (any of ($str*))
}
```

Rule IronTiger_Gh0stRAT_variant

```
rule IronTiger_Gh0stRAT_variant
{
	meta:
		author="Cyber Safety Solutions, Trend Micro"
```

```
                comment="This is a detection for a s.exe variant seen in Op. Iron Tiger"

        strings:
                $mz="MZ"

                $str1="Game Over Good Luck By Wind" nocase wide ascii
                $str2="ReleiceName" nocase wide ascii
                $str3="jingtisanmenxiachuanxiao.vbs" nocase wide ascii
                $str4="Winds Update" nocase wide ascii

        condition:
                $mz at 0 and (any of ($str*))
}
```

Rule IronTiger_GTalk_Trojan

```
rule IronTiger_GTalk_Trojan
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"

                $str1="gtalklite.com" nocase wide ascii
                $str2="computer=%s&lanip=%s&uid=%s&os=%s&data=%s" nocase wide ascii
                $str3="D13idmAdm" nocase wide ascii
                $str4="Error: PeekNamedPipe failed with %i" nocase wide ascii

        condition:
                $mz at 0 and (2 of ($str*))
}
```

Rule IronTiger_HTTPBrowser_Dropper

```
rule IronTiger_HTTPBrowser_Dropper
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"
        strings:
                $mz="MZ"

                $str1=".dllUT" nocase wide ascii
                $str2=".exeUT" nocase wide ascii
                $str3=".urlUT" nocase wide ascii

        condition:
                $mz at 0 and (2 of ($str*))
}
```

Rule IronTiger_HTTP_SOCKS_Proxy_soexe

```
rule IronTiger_HTTP_SOCKS_Proxy_soexe
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"

                $str1="listen SOCKET error." nocase wide ascii
                $str2="WSAAsyncSelect SOCKET error." nocase wide ascii
                $str3="new SOCKETINFO error!" nocase wide ascii
                $str4="Http/1.1 403 Forbidden" nocase wide ascii
                $str5="Create SOCKET error." nocase wide ascii

        condition:
                $mz at 0 and (3 of ($str*))
}
```

Rule IronTiger_NBDDos_Gh0stvariant_dropper

```
rule IronTiger_NBDDos_Gh0stvariant_dropper
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"
                $str1="This service can't be stoped." nocase wide ascii
                $str2="Provides support for media palyer" nocase wide ascii
                $str4="CreaetProcess Error" nocase wide ascii

                $bla1="Kill You" nocase wide ascii
                $bla2="%4.2f GB" nocase wide ascii

        condition:
                $mz at 0 and ((any of ($str*)) or (all of ($bla*)))
}
```

Rule IronTiger_PlugX_DosEmulator

```
rule IronTiger_PlugX_DosEmulator
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"

                $str1="Dos Emluator Ver" nocase wide ascii
                $str2="\\PIPE\\FASTDOS" nocase wide ascii
                $str3="FastDos.cpp" nocase wide ascii
                $str4="fail,error code = %d." nocase wide ascii

        condition:
                $mz at 0 and (any of ($str*))
}
```

Rule IronTiger_PlugX_FastProxy

```
rule IronTiger_PlugX_FastProxy
{
        meta:
                author="Cyber Safety Solutions, Trend Micro"

        strings:
                $mz="MZ"
```

```
			$str1="SAFEPROXY HTServerTimer Quit!" nocase wide ascii
			$str2="Useage: %s pid" nocase wide ascii
			$str3="%s PORT[%d] TO PORT[%d] SUCCESS!" nocase wide ascii
			$str4="p0: port for listener" nocase wide ascii
			$str5="\\users\\whg\\desktop\\plug\\" nocase wide ascii
			$str6="[+Y] cwnd : %3d, fligth:" nocase wide ascii

		condition:
			$mz at 0 and (any of ($str*))
}
```

Rule IronTiger_PlugX_Server

```
rule IronTiger_PlugX_Server
{
		meta:
			author="Cyber Safety Solutions, Trend Micro"

		strings:
			$mz="MZ"

			$str1="\\UnitFrmManagerKeyLog.pas" nocase wide ascii
			$str2="\\UnitFrmManagerRegister.pas" nocase wide ascii
			$str3="Input Name..." nocase wide ascii
			$str4="New Value#" nocase wide ascii
			$str5="TThreadRControl.Execute SEH!!!" nocase wide ascii
			$str6="\\UnitFrmRControl.pas" nocase wide ascii
			$str7="OnSocket(event is error)!" nocase wide ascii
			$str8="Make 3F Version Ok!!!" nocase wide ascii
			$str9="PELEASE DO NOT CHANGE THE DOCAMENT" nocase wide ascii
			$str10="Press [Ok] Continue Run, Press [Cancel] Exit" nocase wide ascii

		condition:
			$mz at 0 and (2 of ($str*))
}
```

Rule IronTiger_ReadPWD86

```
rule IronTiger_ReadPWD86
{
	meta:
		author="Cyber Safety Solutions, Trend Micro"

	strings:
		$mz="MZ"

		$str1="Fail To Load LSASRV" nocase wide ascii
		$str2="Fail To Search LSASS Data" nocase wide ascii
		$str3="User Principal" nocase wide ascii

	condition:
		$mz at 0 and (all of ($str*))
}
```

Rule IronTiger_Ring_Gh0stvariant

```
rule IronTiger_Ring_Gh0stvariant
{
	meta:
		author="Cyber Safety Solutions, Trend Micro"

	strings:
		$mz="MZ"

		$str1="RING RAT Exception" nocase wide ascii
		$str2="(can not update server recently)!" nocase wide ascii
		$str4="CreaetProcess Error" nocase wide ascii

		$bla1="Sucess!" nocase wide ascii
		$bla2="user canceled!" nocase wide ascii

	condition:
		$mz at 0 and ((any of ($str*)) or (all of ($bla*)))
}
```

Rule IronTiger_wmiexec

```
rule IronTiger_wmiexec
{
meta:
        author="Cyber Safety Solutions, Trend Micro"
        comment="wmi.vbs detection"

strings:
        $str1="Temp Result File , Change it to where you like" nocase wide ascii
        $str2="wmiexec" nocase wide ascii
        $str3="By. Twi1ight" nocase wide ascii
        $str4="[both mode] ,delay TIME to read result" nocase wide ascii
        $str5="such as nc.exe or Trojan" nocase wide ascii
        $str6="+++shell mode+++" nocase wide ascii
        $str7="win2008 fso has no privilege to delete file" nocase wide ascii

condition:
        2 of ($str*)
}
```

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey
to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003