FighterPOS Pos Malware Gets Worm Routine

Appendix

TrendLabs Security Intelligence Blog

Jay Yaneza and Erika Mendoza
Trend Micro Cyber Safety Solutions Team

February 2016

Related URLs:

C&C Server for Floki Intruder (WORM_POSFIGHT.SMFLK)

zxcvbnm001[.]xyz
dotodoto1[.]xyz
lkjhgfdsa[.]xyz
poiuytre[.]net

SHA-1:

Detection	SHA1
WORM_POSFIGHT.SMFLK	9506c2586b885be6997c9c6a81c8f155bcebd0d4
	f6a6560f015fc88ae83530400b90c6135bf7b5f0
	27a2bc8aa072456d1ffbb40f2fa6b46bde2ab529
	d9e9d84f927ca09d4b3b8ca80c2a977eddedd12f
	6f3ec924fb3e3c1927a2fca8f9ca8fb5b2adf953
	1bb006fb04b99fe34eeac36d5834a6b32e78f4a3
	340bfccdf6e8604d123cc322b61092ac5df7ba64
	2c089ed610abada207dd71df3d0f51080f1af3e6
	44df15c0833fd83265e476e8363da5bf40d0bbed
	03b664ff521c7ffa07d9ef171505455f98a3a5a8
	4d24a472483c07041b4d1231199cb540f4e64628
	35a054054a9968f69cf48bfabefae171f0da1f84
	9af08a580732557274fe0e5c79bd86a47287ce19
	f84ed095679efb1956d890f7b9f0ec6c3483e2a2
	ba44d5b9699cfcc085759b2b3008b574b67464ef
	0e187566ac885c13daaaf24fd1cf00fb1940997b
	7db5c594710b729ff54bc9dfd8b78e84be30099f
	6558a48e7bd99ea5d1aea237edb76e98e2a4f467
	8b26d40f5b5ce8f4e8d73357f89a1be30f04b873
	5324ed908aa38b8711ed20229a9e7d0f4d9ea519
	01275643b9a8b69ad977ab04abc97172e3ff6e0c
	97c957163f1b333f25ae39f3199f3d1a0c6f86ef
	10a25a7f231bac3d11986461a730ace731f7ae04
	0186f2e403c55feb191b1f3ffc85da5162ce8651
	9f47c91596c4cb47e5c1528b499dbb5fd1763d51
	e85fa46462e760d8da5dd95b4488900f752b4b02
	03d618ceeb3d9aa493a8350b304ed4dd38fb42ca
	aa445acf0bdbcc13a93825f8fe35bcf5bafd2e1c
	6d7ef976a2ef129f8d8d644afa0be01078d7febf
	e9ff16b725e1e903f8f93922c86ab23b4cfc593e
	40af7c037af254fd8a6a2ac0975a3747ec4c93d5

Detection	SHA1
	108fca73e6806c5738d0ababe77e1afe76f71b52
	7b30c5cf90818eff0b47df63df4ea65fce23d48f
	0e4b37283051fa39499b8b012d3f322a46e5b8e3
	0f9aa1a64f9c76a96d9941f24667bf78d4409232
TSPY_POSFIGHT.F	5c4b3918f339a8d1d365eace8036db25d7fcb989
	0cdc60f72bed97e7043b6fa0377f009519874860
	7f349f7bef2e79b4ac623a5311fb542d0b0492e8
	6bcb1815b754d576866545626e655c5ebc87f50b
	df969e545acc4df1fcd1a5f2b61ae9c73600c129
	2f55c67dd47e7a1e768cc3a50584ddd1d69ce664
Tools (HKTL_POSRECORD)	eade94261ac7dd28a1df7943ded41cea6a4899a8
	e1378f25090642dec0a52c9c29aba00db5c05fba
	7b3977276fb876da2f3cb136762f613832aad7cb
	a631eb3b67bf38a603c6c90dfae5ec19cee67a14

Yara Rules:

The following is the YARA rule for this threat. Note that the rules PoS_Malware_MainBinary, PoS_Malware_MainBinary1 and PoS_Malware_FlokiIntruder takes advantage of YARA's capability reference the rule PoS_Malware_ActiveComponent.

```
rule PoS_Malware_ActiveComponent : FighterPOS
{
	meta:
		description = "RAM scrapper component used by FighterPOS"
		author = "Trend Micro, Inc"
	strings:
		$pdb = /:\\users\\tom\\.{20,200}scan\.pdb/ nocase
	condition:
		$pdb
}

rule PoS_Malware_MainBinary : FighterPOS
{
	meta:
		description = "Main FighterPOS infector, with ActiveComponent as
resource"
		author = "Trend Micro, Inc"
	strings:
		$string1 = "BrFighter"
		$string2 = "bot/dumper.php?id="
		$string3 = "bot/keylogger.php?id="
		$string4 = "\\Users\\avanni\\"
	condition:
		(any of ($string*)) and PoS_Malware_ActiveComponent
}
```

```
rule PoS_Malware_MainBinary1 : FighterPOS
{
	meta:
		description = "Main FighterPOS infector, without ActiveComponent as
resource"
		author = "Trend Micro, Inc"
	strings:
		$string1 = "BrFighter"
		$string2 = "bot/dumper.php?id="
		$string3 = "bot/keylogger.php?id="
		$string4 = "\\Users\\avanni\\"
	condition:
		(any of ($string*)) and not PoS_Malware_ActiveComponent
}

rule PoS_Malware_FlokiIntruder : FighterPOS
{
	meta:
		description = "Main FighterPOS infector, with ActiveComponent as
resource. FlokiIntruder release."
		author = "Trend Micro, Inc"
	strings:
		$string1 = "FlokiIntruder"
		$string2 = "bot/dumper.php" wide
		$string3 = "bot/key.php" wide
		$users1 = "\\Users\\UserPC\\" wide
		$users2 = "\\Users\\root\\" wide
	condition:
		(all of ($string*)) and (any of ($users*)) and
PoS_Malware_ActiveComponent
}

rule PoS_Malware_ TSPY_POSFIGHT.F: FighterPOS
{
	meta:
		author = "Trend Micro, Inc"
		description = "FighterPOS modification, using TSPY_POSFIGHT.B OR
TSPY_POSLOGR.SMY for scraping"
	strings:
		$string0 = "Software\\Borland\\Locales"
		$string1 = "SOFTWARE\\Borland\\Delphi\\RTL"
		$string2 = "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
		$string3 = "JavaWT"
		$string4 = "%s.Seek not implemented$Operation not allowed on sorted list"
wide
		$string5 = "Toolhelp32ReadProcessMemory"
		$string6 = "VBWYT-BBWKV-P86YX-G642C-3C3D3"
		$string7 = "svchost.exe"
	condition:
		all of them
}

rule PoS_Malware_EMVDataRecorder : FighterPOS
{
	meta:
		description = "MSR 2006 EMV recorder by FighterPOS actor"
		author = "Trend Micro, Inc"
	strings:
		$a = "send_apdu -sc 0" wide
		$ = "C:\\GPShell\\data.dat" wide nocase
		$ = "MSVBVM60.DLL" ascii
		$ = "MSR 2006"
	condition:
		#a > 10 and all of them
}
```

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