بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

تحلیل بات‌نت Andromeda

گزارش تحلیلی

شناسه سند ..... MaherReportsTemplate_13990703

نوع سند ..... گزارش تحلیلی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۰۸/۰۳

طبقه‌بندی سند ..... **عادی**

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ مقدمه

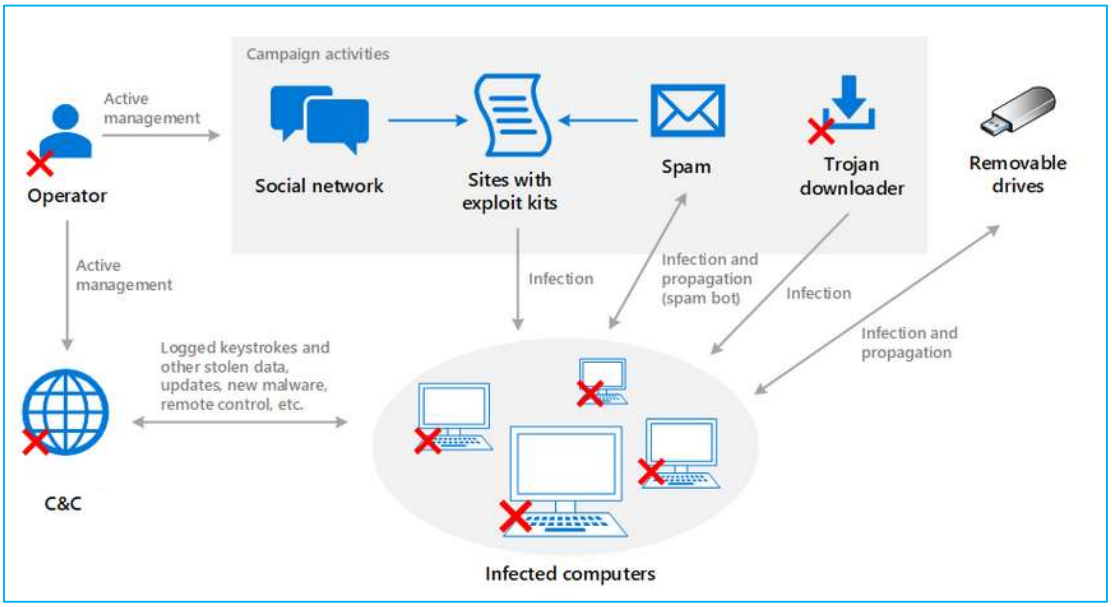
بدافزار Andromeda اولین بار در اواخر سال ۲۰۱۱ مشاهده شده است. این بدافزار با نام win32/Gamarue نیز معروف است. بدافزار Andromeda دارای یک Bot-builder است که با استفاده از این builder و ثبت سرور C&C به راحتی می‌توان نمونه‌های مختلف بات Andromeda را ایجاد کرد. سرور C&C یک برنامه داشبورد مبتنی بر php هست و به مهاجم امکان کنترل و مدیریت بات‌ها را می‌دهد. تعاملات بین بات Andromeda و سرور C&C با استفاده از الگوریتم RC4 رمزگذاری شده است. Andromeda یک بات ماژولار است و از پلاگین-هایی مانند KeyLogger، Rootkit، Socks 4/5، Formgrabber پشتیبانی می‌کند و قابلیت آن با افزودن پلاگین‌هایی مانند Teamviewer و Spreader افزایش می‌یابد.

۱-۱ فرایند انتشار

از زمان مشاهده اولین نمونه از این بدافزار تاکنون، از روش‌های مختلفی برای توزیع و انتشار این بدافزار استفاده شده، که از معمول‌ترین روش‌های مذکور می‌توان به موارد ذیل اشاره کرد.

- انتشار در بستر پیام‌رسان‌ها و شبکه‌های اجتماعی از قبیل فیس‌بوک (لینک‌هایی که کاربر را به سرورهای حاوی بدافزار Andromeda هدایت می‌کنند، به‌صورت انبوه در سطح این بسترها میان کاربران منتشر گردیده)
- به‌کارگیری بدافزار Andromeda از طریق Exploit-Kitهای مختلف توسط مهاجمان (از قبیل کیت Crime)
- ایمیل‌های اسپم با ضمیمه و پیوست فایل اجرایی Andromeda
- تزریق فایل اجرایی Andromeda به وب‌سایت‌های مختلف و انتقال به سیستم کاربران از طریق Drive-by-Download

هنگامی‌که این بدافزار سیستمی را آلوده کرد، با سرور C&C ارتباط برقرار نموده و سیستم مذکور را به بخشی از شبکه botnet تبدیل می‌کند. از طریق سرور C&C مهاجم قادر است که ماشین‌های آلوده به بدافزار را کنترل کند، اطلاعات را به سرقت ببرد یا دستوراتی را برای بارگیری ماژول‌های مخرب اضافی صادر کند. شکل زیر به‌صورت شماتیک این فرایند را نشان می‌دهد.



شکل ۱- مکانیسم‌های مختلف انتشار بدافزار Andromeda

۲-۱ رفتار Andromeda

بررسی‌های صورت گرفته در آزمایشگاه نشان می‌دهد که این بدافزار به‌محض اجرا در ماشین قربانی، کدهای خود را به یکی از پروسس‌های معمول و جاری سیستم‌عامل خانواده ویندوز تزریق می‌کند. با اجرای این بدافزار تحت پوشش پروسس سیستمی، حیات بدافزار در سیستم قربانی پایدارتر بوده و ارتباط این باتنت با مرکز کنترل و C&C حفظ می‌گردد که در این مرحله C&C با ارسال سایر ماژول‌ها و فایل‌های مخرب به سیستم آلوده، فرآیند آلوده‌سازی را تکمیل می‌کند. Andromeda برای اینکه با خاموش شدن سیستم قربانی، حیات خود را همچنان حفظ نماید، یک نمونه از فایل اجرایی خود را در مسیر Local Setting سیستم قربانی قرار داده و مسیر و نام این فایل را به مسیر مشخصی از Registery اضافه می‌کند.

۲ شرح تحلیل

همان‌طور که قبلاً اشاره شد، Andromeda دارای builder هست که نمونه بدافزار Andromeda را ایجاد می‌کند جدول ۱ مشخصات کلی Bot-Builder این فایل ارائه می‌گردد.

جدول ۱- مشخصات Bot-builder باتنت Andromeda

BE31DEDE2DF4BA25EEB71B191A3512BA	هش md5
0D6EF1E4662EB0D624A395AFE3E8C16A5F57BE4D	هش SHA1
2089C3234F1808F2F729407FBEC57E42F0CAE79590B7E386B8EE2E18E0252F97	هش SHA256

زمان کامپایل	Tue Nov 20 01:12:47 2012
حجم فایل	1373184 bytes
آنتروپی کلی فایل	6.861
تعداد Sectionها	5

در ادامه گزارش، با در نظر گرفتن دو نوع تحلیل ایستا و تحلیل پویا به بررسی ساختار و رفتار نمونه فایل اجرائی Andromeda پرداخته می‌شود.

۲-۱ تحلیل استاتیک

۲-۱-۱ مشخصات فایل

جدول ۲ مشخصات کلی نمونه فایل بدافزاری که با builder مربوط به Andromeda تولید می‌گردد را، نشان می‌دهد.

جدول ۲- مشخصات نمونه بدافزار Andromeda

هش md5	C4741DB4A345A8FA3FFF726746B7A3C6
هش SHA1	D6C6AFEEE2CBA312FDD3E489F07491916E6A4B90
هش SHA256	0B6FA6E5605EED9115D638A3204E014EBC010AFCBFBE809C8582DE4B1931C515
زمان کامپایل	Mon Nov 12 18:39:59 2012
حجم فایل	13824 bytes
آنتروپی کلی فایل	7.693
تعداد Sectionها	1

۲-۱-۲ بخش‌های مختلف فایل

جدول ۳ جزئیات تنها Section نمونه بدافزار Andromeda را نشان می‌دهد.

جدول ۳- جزئیات Section نمونه بدافزار Andromeda

ردیف	نام	آدرس مجازی	اندازه مجازی	اندازه خام	آنتروپی	مشخصات
1	.text	0x00001000	13015 bytes	13312 bytes	7.759	Writable , executable

وجود قابلیت اجرا و نوشتن هم‌زمان در یک بخش و همچنین مقدار بالای هفت آنتروپی، دگردیسی و چندریختی و احتمال رفتار غیرعادی، فایل را نشان می‌دهد.

۲-۱-۳ رشته‌های استخراج‌شده از ساختار فایل

جدول ۴ برخی رشته‌های به‌دست‌آمده از نمونه فایل Andromeda را نمایش می‌دهد.

جدول ۴- برخی از رشته‌های بکار گرفته‌شده در Andromeda

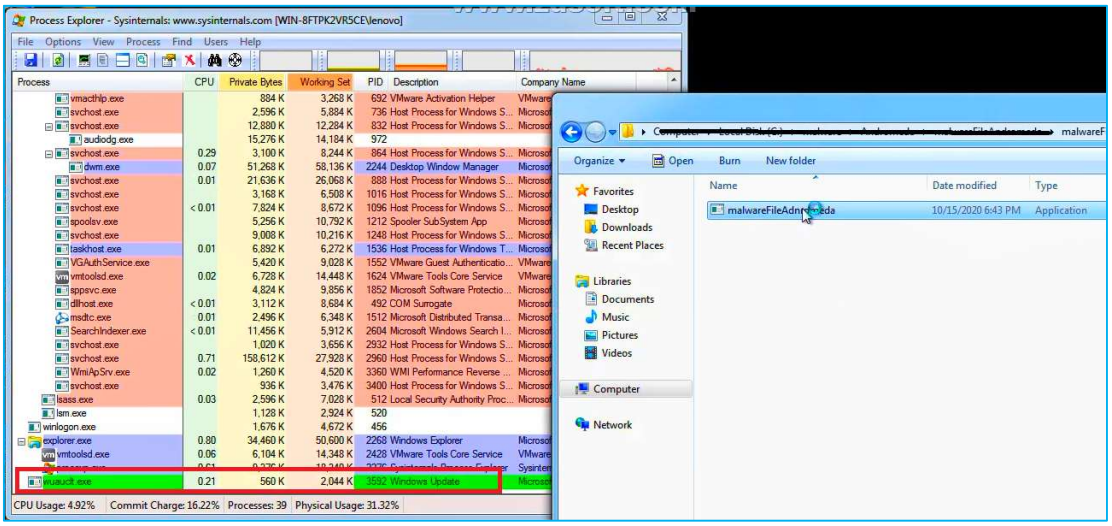
Strings in Andromeda Sample	
!This program cannot be run in DOS mode.	Hajn
kernel32.dll	sMJI
.text	08X.daHtq
9A;M	d40e
hlol	af7$RnpK
hdll	SVW9jdp
hdll.hsbie	2 hT
h.dllhpi32hadva	p,@4ZA'NW"
hnum	imyo
hsk\ehs\dihviceh\serhlsethntrohntcohurrehem\chsyst	MGiI
PQQQR	QRVq
tLj0	ABCDEFG
wmwat9	HIJKLMNO`PzSTUV
vboxt-	WXYZabcd
qemut!	efghijkl
nxdMPv	mnopqrst
NtDela	uvwxyz01
cubion	23456789'+/
MapV	SWVCE
ceqs	/%s

۲-۲ تحلیل دینامیک

فایل اجرائی Andromeda در محیط آزمایشگاهی و در سناریوهای مختلف شبیه‌سازی برای C&C تحت سیستم‌عامل‌های ویندوز XP ، ویندوز 7 و لینوکس اجرا گردید. برای بررسی رفتار این بدافزار از ابزارهای مانند Process Explorer ، winDump و RegShot استفاده شده است. البته برای بررسی دقیق‌تر رفتار باتنت Andromeda علاوه بر نمونه فایل بدافزاری که در تحلیل ایستا به آن اشاره شد، ۶۴ نمونه بدافزاری در قالب ۱۱۲ سناریو اجرائی استفاده شده است.

۲-۲-۱ پروسس‌های ایجادشده

بررسی‌ها نشان می‌دهد این بدافزار به‌محض اجرا ، کدهای خود را در یک پروسس قانونی سیستم‌عامل ماشین قربانی تزریق می‌کند و برای حفظ حیات خود از تکنیک تزریق متقابل[۱] استفاده می‌کند. شکل ۲ نشان می‌دهد که به‌محض اجرای بدافزار پروسس wuauclt.exe اجرا می‌گردد.



شکل ۲- اجرای wuauclt.exe توسط Andromeda

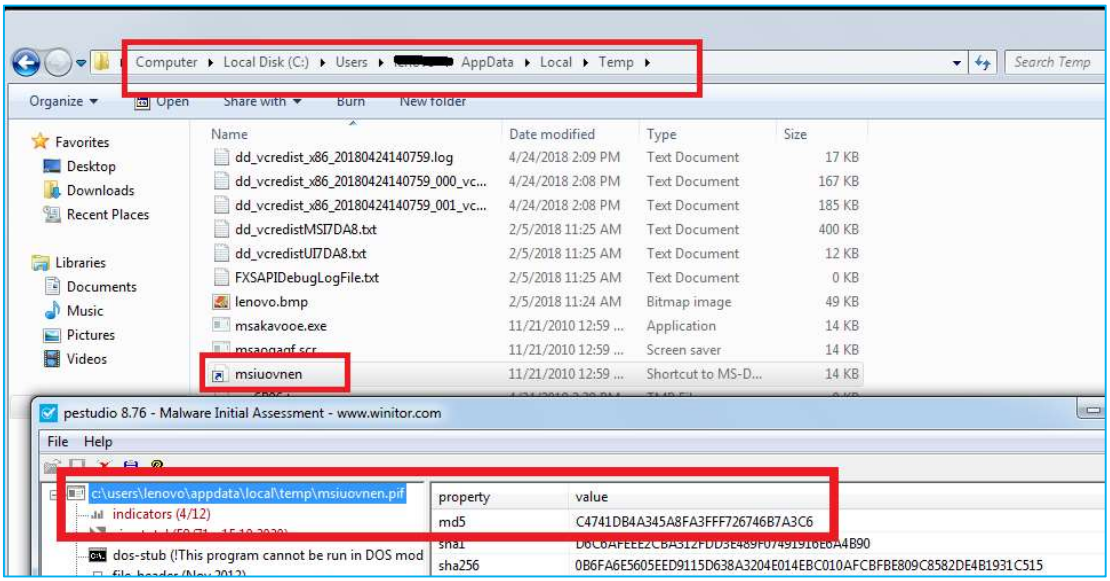
بررسی نمونه‌های دیگر بدافزار andromeda در سناریوهای مختلف نشان می‌دهد که این بدافزار علاوه بر پروسس wuauclt.exe ، از پروسس‌های زیر نیز برای حفظ حیات خود استفاده می‌کند.

- msiexec.exe
- wupgrade.exe
- svchost.exe

۲-۲-۲ تغییرات سطح فایل

بررسی‌ها نشان می‌دهد Andromeda با استفاده از پروسسی که کد خود را در آن تزریق نموده، کپی از خود را در مسیر c:\Users\admin\AppData\Local\Temp قرار می‌دهد. نام این فایل در سناریوهای مختلف یک نمونه بدافزار Andromeda متفاوت دیده‌شده است. شکل ۳ نمونه فایل کپی شده در این مسیر را نشان می‌دهد.

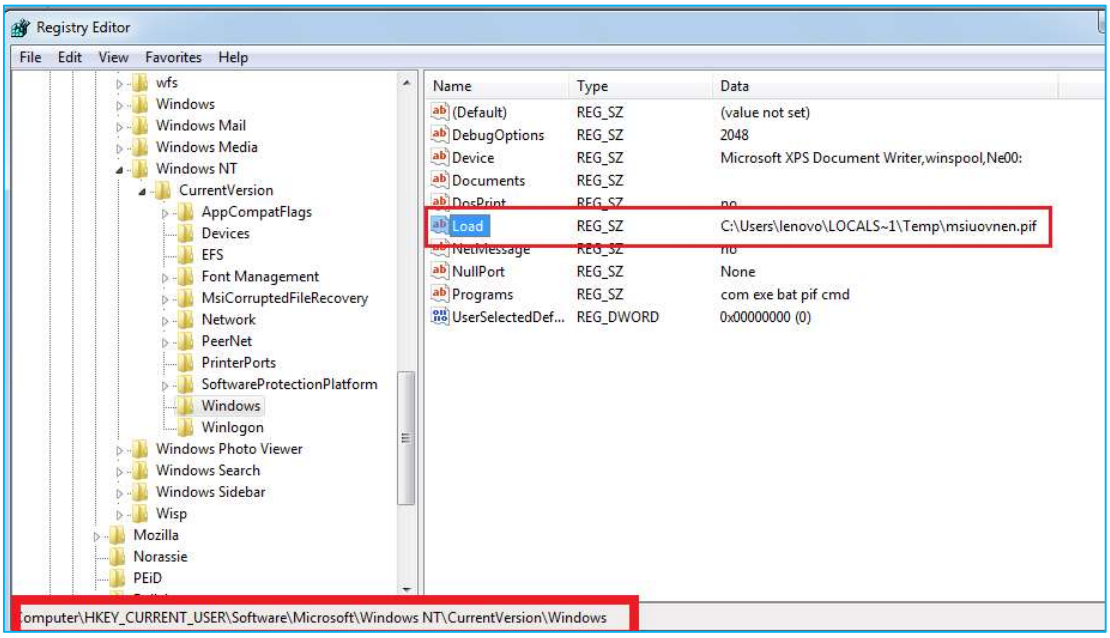
[۱] Cross Process Injection



شکل ۳- کپی فایل بدافزار Andromeda در مسیر Local Setting سیستم قربانی

۳-۲-۲ تغییرات سطح رجیستری

Andromeda برای حفظ حیات خود بعد از restrat شدن سیستم قربانی، مقدار کلید رجیستری load را در مسیر رجیستری HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows به فایل ایجادشده در مسیر Local Setting سیستم قربانی ست می‌کند. بدین ترتیب با boot شدن سیستم قربانی، بدافزار به‌واسطه مقدار این کلید، مجدد اجرا می‌شود. شکل ۴ مقدار کلید رجیستری load را در مسیر رجیستری فوق، نمایش می‌دهد.



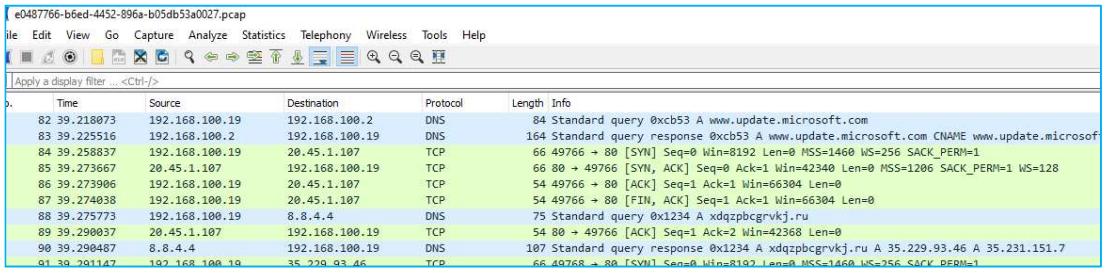
شکل ۴- ست شدن مقدار کلید رجیستری load به کپی فایل بدافزاری Andromeda

۴-۲-۲ تغییرات در سطح شبکه

برای به دست آوردن تغییرات سطح شبکه Andromeda، نمونه‌های مختلفی از این بدافزار در قالب چندین سناریوی اجرایی، مورد بررسی قرارگرفته است. نتایج مشاهده شده به شرح زیر است:

- ارتباط با C&C با استفاده از پروتکل TCP با ارسال بسته‌های SYN .

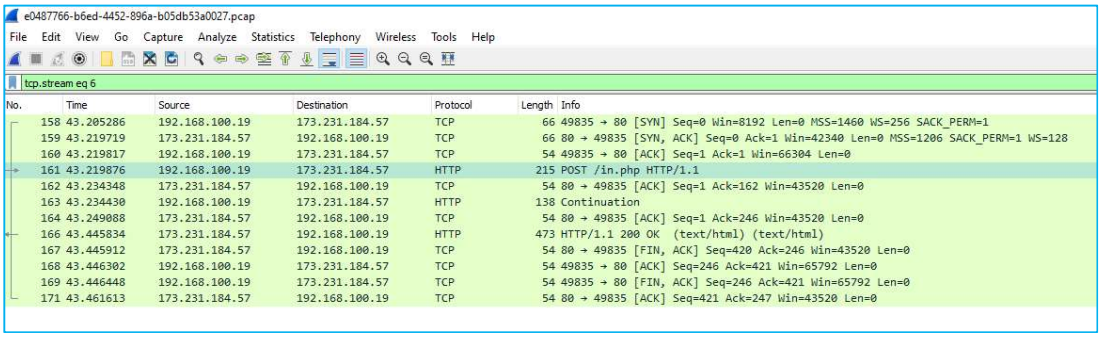
شکل ۵ نمونه‌ای از این ارتباط را دریکی از سناریوهای مورد بررسی نشان می‌دهد.



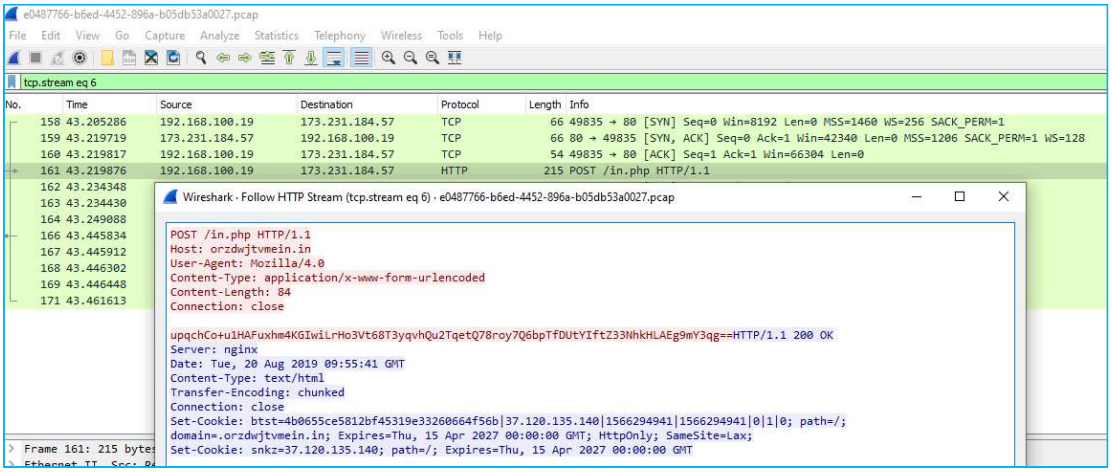
شکل ۵-ارتباط با C&C با بسته‌های SYN

- برقراری ارتبط باتنت با C&C با استفاده از پروتکل HTTP و کدگذاری برخی از محتواهای مبادلاتی میان باتنت و C&C

شکل ۶ و ۷ نمونه‌ای از این ارتباط را نشان می‌دهد.



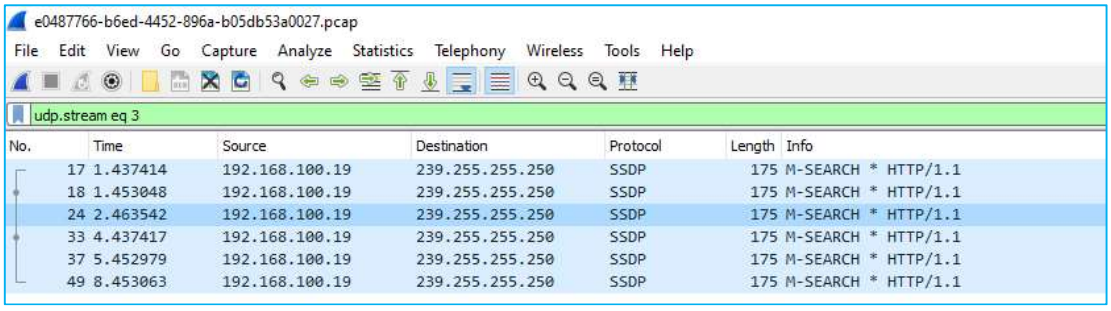
شکل ۶- نمونه‌ای از بسته‌های ارسالی موجود در یکی از سناریوهای مورد بررسی



شکل ۷- محتوای بسته

- ارسال بسته‌های UDP مرتبط با پروتکل SSDP و به‌کارگیری آدرس MultiCast، 239.255.255.250 جهت شناسایی سرویس‌های فعال در طول شبکه داخلی سیستم آلوده‌شده

شکل ۸ نمونه‌ای از این ارتباط را نمایش می‌دهد.



شکل ۸- بسته‌های UDP ، Multicast شده

جدول ۵ آدرس‌های IP مشاهده شده را، در بررسی نمونه‌های بدافزاری Andromeda در سناریوهای مختلف نمایش می‌دهد.

جدول ۵ – آدرس‌های IP مشاهده شده در سناریوهای مختلف شبیه‌سازی‌شده

آدرس‌های IP		
52.50.65.32	77.222.62.31	2.16.186.24
62.76.187.171	82.145.215.40	13.64.25.102
62.113.202.81	85.143.166.119	13.77.161.179
63.251.235.88	93.184.216.34	13.107.21.200
65.55.50.189	93.184.220.29	20.41.46.145
65.55.50.158	104.215.148.63	20.45.1.107
66.225.197.197	104.42.225.122	34.198.126.16
71.209.247.2	104.111.238.86	34.98.99.30
71.223.68.37	134.170.58.222	35.229.93.46
72.26.218.79	141.8.194.74	35.231.151.7
72.26.218.77	148.81.111.121	37.139.47.56
74.220.199.9	153.92.0.100	40.91.124.111
178.218.222.185	162.217.99.136	40.70.224.146
184.105.192.2	172.217.21.195	40.90.247.210
185.26.182.93	172.217.23.164	40.67.189.14
192.42.116.41	173.231.184.57	40.112.72.205
194.58.119.193	173.231.189.24	209.141.38.71
195.123.219.192	176.58.104.168	216.58.210.3
204.79.197.200	206.189.61.126	216.58.214.99
204.11.56.48	208.100.26.245	216.58.214.110

جدول ۶ بخشی از Url های مشاهده شده را، در بررسی نمونه‌های بدافزاری Andromeda در سناریوهای مختلف نمایش می‌دهد.

جدول ۶ – بخشی از Urlهای مشاهده‌شده

بخشی از url های مشاهده شده در سناریوهای مختلف
• http://finley.su/se/gate.php • http://bighecks.net/http/image.php • http://sonic4us.ru/http/image.php • http://morphed.ru/static.php

- http://amnsreiuojy.ru/2ldr.php
- http://62.76.187.171/srt/404.php
- http://37.139.47.56/srt/404.php
- http://85.143.166.119/srt/404.php
- http://pronto.estercrocetta.it/new_and/Zjs93jLSk.php
- http://jarkijden.com/and/image.php
- http://retinamac.ru/and/image.php
- http://go.microsoft.com/fwlink/?LinkId=57426&Ext=buj
- http://shell.windows.com/fileassoc/fileassoc.asp?Ext=buj
- http://filer.comeze.com/panel/image.php
- http://ordering-checks.com/round1/image.php
- http://sonic4us.ws/login/gate.php
- http://dvdonlinestore.net/opreationday1/image.php
- http://dnshkjashkd1.ru/and/gate.php

۳ فرآیند شناسایی و پاک‌سازی Andromeda

شکل زیر وضعیت تشخیص فایل مورد بررسی را در ویروس‌توتال نشان می‌دهد. در این سامانه از بین ۷۱ موتور آنتی‌ویروس فعال، ۵۹ موتور قادر به شناسایی فایل بعنوان یک فایل بدافزار شده‌اند

شکل ۹= وضعیت تشخیص فایل در ویروس توتال

شکل ۱۰ اسامی موتورهای آنتی‌ویروس را که فایل بدافزاری Andromeda را تشخیص داده‌اند، را نمایش می-دهد.

Acronis	Suspicious	Ad-Aware	Gen:Variant.Ser.Razy.7042
AhnLab-V3	Backdoor/Win32.Androm.R41944	ALYac	Gen:Variant.Ser.Razy.7042
Antiy-AVL	Trojan[Backdoor]/Win32.Androm.a	SecureAge APEX	Malicious
Arcabit	Trojan.Ser.Razy.D1B82	Avast	Sf:Citadel-A [Trj]
AVG	Sf:Citadel-A [Trj]	Avira (no cloud)	WORM/Gamarue.itza
BitDefender	Gen:Variant.Ser.Razy.7042	BitDefenderTheta	AI:Packer.2E3E93F71E
Bkav	W32.Msbzmu.Trojan	CAT-QuickHeal	Worm.Gamarue.I1
ClamAV	Win.Trojan.Gamarue-6986405-0	Comodo	TrojWare.Win32.Kryptik.AFJS@4p06v2
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.4a345a
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Andromeda.A.gen!Eldorado	DrWeb	BackDoor.Andromeda.22
eGambit	Unsafe.AI_Score_99%	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ser.Razy.7042 (B)	eScan	Gen:Variant.Ser.Razy.7042
ESET-NOD32	Win32/TrojanDownloader.Wauchos.A	F-Secure	Worm.WORM/Gamarue.itza
FireEye	Generic.mg.c4741db4a345a8fa	Fortinet	W32/Citadel.A!tr
GData	Gen:Variant.Ser.Razy.7042	Ikarus	Backdoor.Win32.Androm
Jiangmin	Backdoor/Androm.ag	K7AntiVirus	Trojan (00536d121)
K7GW	Trojan (00536d121)	Kaspersky	Backdoor.Win32.Androm.a
Malwarebytes	Trojan.Agent.NR	MAX	Malware (ai Score=80)
MaxSecure	Backdoor.Androm.a	McAfee	W32/Worm-FFE!C4741DB4A345
McAfee-GW-Edition	BehavesLike.Win32.Generic.lc	Microsoft	Worm:Win32/Gamarue.I
NANO-Antivirus	Virus.Win32.Gen.ccmw	Qihoo-360	HEUR/QVM19.1.9ABB.Malware.Gen
Rising	Worm.Win32.Gamarue.b (CLASSIC)	SentinelOne (Static ML)	DFI - Suspicious PE
Sophos AV	Troj/Gamarue-AG	Sophos ML	ML/PE-A + Troj/Gamarue-AG
SUPERAntiSpyware	Trojan.Agent/Gen-Cryptic	Symantec	Downloader.Dromedan
TACHYON	Backdoor/W32.Androm.13824.I	Tencent	Backdoor.Win32.Androm.a
TrendMicro	BKDR_ANDROM.SMV1	TrendMicro-HouseCall	BKDR_ANDROM.SMV1
VBA32	BScope.Backdoor.Androm	VIPRE	Trojan-Downloader.Win32.Dofoil.a (v)
ViRobot	Backdoor.Win32.A.Androm.13824.X	Webroot	W32.Trojan.Dantmil
ZoneAlarm by Check Point	Backdoor.Win32.Androm.a	Lastline	MALWARE TROJAN

شکل ۱۰- اسامی موتورهای آنتی‌ویروس تشخیص‌دهنده بدافزار Andromeda

بررسی‌ها نشان می‌دهد که آنتی‌ویروس پادویش و سامانه سَتفا (که جزء موتورهای تشخیص‌دهنده بومی بدافزار هستند) امکان شناسایی بات‌نت Andromeda را دارند.

برای پاک‌سازی End-Sytem آلوده‌شده به Andromeda، می‌توان یکی از آنتی‌ویروس‌های فوق را نصب و ویژگی محافظت مستمر (Real Time Protection) آن را فعال نمود. بدین ترتیب بدافزار ابتدا "منع دسترسی" شده و سپس "حذف" می‌گردد.

۳-۱ راهکار دستی برای پاک‌سازی از سیستم قربانی

برای حذف بدافزار Andromeda به‌صورت دستی مراحل زیر را اجرا نماید:

۱- نام پروسسی که باتنت andromeda، کدهای خود را در آن تزریق نموده در Task Manager بیابید. (اسامی این پروسس‌ها قبلاً در تحلیل پویا ذکرشده گردید.)

۲- از طریق برنامه Run در سیستم‌عامل خانواده ویندوز و با استفاده از دستور regedit، رجیستری سیستم را باز نموده و در مسیر رجیستری HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows مقدار کلید رجیستری load را به دست آوردید. مقدار این کلید رجیستری نام فایل بدافزاری است که کپی و رونوشتی از فایل اصلی بوده و باعث می‌شود که سیستم قربانی به‌محض log in شدن، مجدداً اجرا گردد.

۳- به مسیر Local Setting (AppData/local/temp) مراجعه کرده و فایل بدافزاری را پاک نماید.

۴ IoC[۲] مستخرج از تحلیل استاتیک و دینامیک Andromeda

در این بخش مشخصه و ویژگی‌های منحصربه‌فرد بدافزار Andromeda که از تحلیل استاتیک و دینامیک این بدافزار در آزمایشگاه استخراج شده است، ارائه می‌شود که این مشخصه‌ها با این هدف استخراج گردیده که به‌صورت کاملاً عملیاتی و کاربردی، با به‌کارگیری آن‌ها چه در سطح سیستم کاربران (End-System) و چه در سطح شبکه سازمان و شرکت‌های مختلف، امکان شناسایی و بلوکه کردن چرخه حیات این باتنت میسر گردد. مشخصه‌های مستخرج در دو سطح سیستم‌عامل و شبکه تقسیم‌بندی شده که مشخصه‌های تحت شبکه منجر به شناسایی باتنت Andromeda از طریق بسته‌های مبادلاتی این بدافزار با مرکز کنترل و C&C آن می‌گردد و مشخصه‌های سطح سیستم‌عامل همان‌طور که پیش‌تر نیز بررسی گردید، غالباً در هسته و موتور آنتی‌ویروس-های معتبر و به‌روزرسانی شده موجود می‌باشند، که منجر به شناسایی و پاک‌سازی بدافزار Andromeda می‌گردند.

لازم به ذکر است با توجه به اینکه در طول تحلیل نمونه‌های مختلف جمع‌آوری‌شده از باتنت Andromeda، آدرس IP مرکز کنترل و C&C استخراج‌شده از هرکدام از نمونه‌ها غالباً متفاوت و مجزا از سایر نمونه‌ها بود،

[۲] Indicators of Compromise

لذا لحاظ نمودن آدرس‌های IP مرکز کنترل و C&C به‌عنوان مشخصه و ویژگی تشخیص‌دهنده برای باتنت Andromeda غیرکاربردی بوده و به‌عنوان IoC مدنظر قرار نگرفت.

۱-۴ IoC و مشخصه‌های شناسایی باتنت Andromeda در طول شبکه

شاخصه‌های منحصربه‌فرد باتنت Andromeda در قالب جدول ۷ نشان داده است که این IoC و مشخصه‌ها در قالب Rule و الگوهای استاندارد امکان تزریق به سامانه‌های IDS/IPS و UTM جهت شناسایی و Drop بسته-های حاوی این مقادیر را خواهند داشت تا چرخه حیات و ارتباط این باتنت با مرکز کنترل و C&C قطع شود.

جدول ۷- IoC مستخرج از باتنت Andromeda تحت شبکه

ردیف	نوع بسته	جهت ارسال بسته	محتوای بسته در قالب Hexadecimal	شرح IoC
۱	TCP	از سمت باتنت به سرور CnC	|47 45 54 20| |5F 57| |2E| |2f 70 75 62 6c 69 63 6b 65 79 2f| ! |41 63 63 65 70 74 3A| ! |43 6F 6E 6E 65 63 74 69 6f 6E 3A| ! | 52 65 66 65 72 65 72 3A|	بسته TCP حاوی مقادیر "GET/" و "_W" و "-" و "/publickey/" بوده و فاقد مقادیر "Accept:" و "Connection:" و "Referer:" باشد (این بسته در خصوص محتوای Header و سرآیند درخواست http باتنت Andromeda به CnC است.)
۲	TCP	از سمت سرور CnC به باتنت	| 79 78 30 3d 30 3b 79 78 31 3d 31 3b 79 78 32 3d 32 3b 79 78 33 3d 33 3b 79 78 34 3d 34 3b 79 78 35 3d 35 3b 79 78 36 3d 36 3b 79 78 37 3d 37 3b 79 78 38 3d 38 3b 79 78 39 3d 39 3b 6c 69 74 3d 22 22 | | 66 75 6e 63 74 69 6f 6e 20 46 69 6e 64 50 72 6f 78 79 46 6f 72 55 52 4c 28 75 72 6c 2c 20 68 6f 73 74 29|	بسته TCP حاوی مقادیر "function FindProxyForURL(url, host)" و "yx0=0;yx1=1;yx2=2;yx3=3;yx4=4;yx5=5; yx6=6;yx7=7;yx8=8;yx9=9;lit""" باشد. (این دو مورد در طول پاسخ‌های http ارسالی از سمت CnC مشاهده می‌گردد.)
۳	TCP	از سمت باتنت به سرور CnC	|2f 66 6f 72 75 6d 2e 70 68 70|	بسته TCP حاوی مقادیر "forum.php/" و "User-Agent: Mozilla/4.0"

			55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 0D 0A|	"/" بوده و فاقد مقادیر "Accept" و "Referer" باشد. (این بسته در خصوص محتوای Header و سرآیند درخواست http باتنت Andromeda به CnC است.)
۴	TCP	از سمت باتنت به سرور CnC	| 2e 6d 6f 64 | | 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 0D 0A| و عبارت منظم: /[a-z]{2}_[a-z0-9]{8}\.mod/Ui این عبارت منظم که با سینتکس PCRE[۳] نگاشته شده است، به این معنی است که هر رشته‌ای که ابتدا دو کاراکتر از حروف a تا z، سپس کاراکتر underline (_)، سپس هشت مورد از حروف a تا z، سپس کاراکتر dot (.) و در ادامه استرینگ mod را شامل باشد، با این عبارت منظم منطبق است.	بسته TCP حاوی مقادیر ".mod" و "User-Agent: Mozilla/4.0 /" بوده و حاوی محتوایی منطبق با Regular Expression یا عبارت منظم [a-z]{2}_[a-z0-9]{8}\.mod/Ui/ باشد. و فاقد مقادیر "Accept" و "Referer" باشد.
۵	TCP	از سمت CnC به باتنت	| 53 65 72 76 65 72 3a 20 53 74 61 6c 69 6e|	بسته TCP حاوی مقادیر "Server: Stalin" باشد.

[۳] Perl Compatible Regular Expressions

۲-۴ IoC و مشخصه‌های شناسایی باتنت Andromeda در سیستم کاربران

IoC و مشخصه‌های منحصربه‌فرد فایل اجرایی باتنت Andromeda که از تحلیل استاتیک آن استخراج گردیده، در قالب جدول ۸ نشان داده است. موارد ۱، ۲ و ۳ در تمامی نمونه‌های مختلف این باتنت مشاهده گردیده و از میان موارد ۴ تا ۳۶ درصورتی‌که حداقل هفت مورد از آن‌ها در یک فایل اجرایی پلتفرم ویندوز (PE[4]) مشاهده گردد و حجم فایل اجرایی مربوطه کمتر از ۲۰۴۸۰۰ بایت باشد، می‌توان نتیجه گرفت که فایل اجرایی مذکور مخرب بوده و از خانواده باتنت Andromeda است.

به‌کارگیری این مشخصه‌ها در موتور و هسته آنتی‌ویروس‌های مختلف منجر به شناسایی نمونه‌های مختلف این باتنت در سیستم کاربران و End-System گردیده است که در بخش‌های قبل لیستی از آنتی‌ویروس‌هایی که قادر به شناسایی نمونه‌های مختلف این باتنت در سیستم کلاینت و سرور پلتفرم ویندوز هستند، ارائه گردید.

جدول ۸- IoC های استخراج‌شده از تحلیل استاتیک فایل اجرایی Andromeda

ردیف	محتوای ثابت فایل اجرایی باتنت Andromeda در قالب Hexadecimal	محتوای Ascii و OpCode معادل مقادیر هگزادسیمال
۱	| 68 73 6b 5c 5c 65 68 73 5c 5c 64 69 68 76 69 63 65 68 5c 5c 73 65 72 68 6c 73 65 74 68 6e 74 72 6f 68 6e 74 63 6f 68 75 72 72 65 68 65 6d 5c 5c 63 68 73 79 73 74|	"hsk\\ehs\\dihviceh\\serhlsethntrohntcohurrehem\\chsyst"
۲	| 41 70 70 44 61 74 61 5c 5c 4c 6f 63 61 6c 5c 5c 54 65 6d 70 5c 5c 5f 2e 6e 65 74 5f 5c 5c 6d 73 69 65 78 65 63 2e 65 78 65 |	"AppData\\Local\\Temp_.net_\\msiexec.exe"
۳	| 1c 1c 1d 03 49 47 46 |	"---IGF"
۴	3688942800ffffff fec1 7408 43 3b5d0c 74cf	mov byte ptr ss:[eax + ebp - 0x100], dl inc cl je 0xa inc ebx cmp ebx, dword ptr [ebp + 0xc] je 0xfffffd1

[4] Portable Executable

inc al mov dl, byte ptr ss:[eax + ebp - 0x100] add bl, dl mov dh, byte ptr ss:[ebx + ebp - 0x100]	fec0 368a942800ffffff 02da 368ab42b00ffffff	۵
jmp 0xffffffd1 xor eax, eax xor ebx, ebx xor ecx, ecx	ebcf 33c0 33db 33c9	۶
xor ebx, ebx xor ecx, ecx xor edx, edx mov edi, dword ptr [ebp + 0x10] inc al	33db 33c9 33d2 8b7d10 fec0	۷

add bl, dl
mov dh, byte ptr ss:[ebx + ebp - 0x100]
mov byte ptr ss:[eax + ebp - 0x100], dh
mov byte ptr ss:[ebx + ebp - 0x100], dl
add dl, dh
and edx, 0xff
mov dl, byte ptr ss:[edx + ebp - 0x100]
	02da 368ab42b00ffffff
	3688b42800ffffff
	3688942b00ffffff 02d6
	81e2ff000000 368a942a00ffffff
		۸

mov dl, byte ptr ss:[edx + ebp - 0x100] xor byte ptr [ecx + edi], dl inc ecx cmp ecx, dword ptr [ebp + 0x14]	368a942a00ffffff 301439 41 3b4d14	۹
cmp ebx, dword ptr [ebp + 0xc] je 0xffffffd1 jmp 0xffffffd1 xor eax, eax	3b5d0c 74cf ebcf 33c0	۱۰

mov ebp, esp
add esp, 0xffffff00
pushal
mov ecx, 0x40
lea edi, [ebp - 4]
mov eax, 0xfffefdfc
	8bec 81c400ffffff 60 b940000000 8d7dfc b8fcfdfeff	۱۱

pushal - pop ebp - xor ecx, ecx	60 e8???????? 5d 81ed???????? 33c9 کاراکتر ? به این معنی است که این محل از عبارت هگزادسیمال می‌تواند مقادیر مختلفی را در نمونه‌های مختلف فایل اجرایی Andromeda به خود بگیرد.	۱۲
cemp al, 0x41 stge dl test edx, ecx je 6	3c41 0f9dc2 85ca 7404	۱۳

movzx eax, byte ptr [esi + 1] test al, al jns 7 or eax, 0xffffff00	0fb64601 84c0 7905 0d00ffffff	۱۴
lea eax, [ebp - 0x30] push eax push 1 push dword ptr [ebp + 8] - test eax, eax	8d45d0 50 6a01 ff7508 e8???????? 85c0	۱۵
test edx, ecx je 6 add al, 0x20 mov byte ptr [esi], al	85ca 7404 0420 8806	۱۶
push eax - add esp, 0xc push 0x10000 -	50 e8???????? 83c40c 6800000100 e8????????	۱۷

cmp al, 0x5a
setle cl
xor edx, edx
cmp al, 0x41
setge dl
	3c5a 0f9ec1 33d2 3c41 0f9dc2	۱۸

mov al, byte ptr [esi] xor ecx, ecx cmp al, 0x5a setle cl	8a06 33c9 3c5a 0f9ec1	۱۹
push 0x1f40 - mov word ptr [ebp - 0x1e], ax mov dword ptr [ebp - 0x1c], 0 push 0	68401f0000 e8???????? 668945e2 c745e400000000 6a00	۲۰
xor eax, eax lea edi, [ebp - 0x64] mov ecx, 0x44 rep stosb byte ptr es:[edi], al push 0	33c0 8d7d9c b944000000 f3aa 6a00	۲۱
xor eax, eax lea edi, [ebp - 0x64] mov ecx, 0x44 rep stosb byte ptr es:[edi], al push 0	ff35???????? e8???????? 8945fc 83f800 0f8476010000	۲۲
- - mov dword ptr [ebp - 4], eax cmp eax, 0 je 0x17c	ff35???????? e8???????? 8945fc 83f800 0f8476010000	۲۳
mov dword ptr [ebp - 0x10], eax cmp eax, -1	8945f0 83f8ff 7479 6a10 8d45e0 50	۲۴

je push lea push	0x7b 0x10 eax, [ebp - 0x20] eax		
cmp je push push	eax, -1 0x68 5 dword ptr [ebp - 0x10]	83f8ff 7466 6a05 ff75f0	۲۵
mov cmp je push lea -	dword ptr [ebp - 0x10], eax eax, -1 0x7b 0x10 eax, [ebp - 0x20]	8945f8 83f800 0f8458010000 6804010000 ff75f8 68????????	۲۶
push mov add -	ebp ebp, esp esp, -0x74	55 8bec 83c48c e8????????	۲۷
- cmp je lea push	 eax, 0 0x21 eax, [ebp - 0xc] eax	e8???????? 83f800 741f 8d45f4 50	۲۸
mov je or call xor call xor	edi, eax 0xffffffda dword ptr [ebp - 4], 0xffffffff dword ptr [esi + 0x38] dword ptr [ebp + 0xc], eax dword ptr [esi + 0x34] edi, eax	8bf8 74d8 834dfcff ff5638 31450c ff5634 33f8	۲۹
mov call mov mov or imul	byte ptr [ebx], al dword ptr [esi + 0x30] ecx, eax eax, dword ptr [ebp - 0x14] eax, 0x77323bc2 ecx, eax	8803 ff5630 8bc8 8b45ec 0dc23b3277 0fafc8	۳۰
inc mov call imul	dword ptr [ebp + 0x18] byte ptr [ebp + ecx - 0x114], al dword ptr [esi + 0x38] ebx, ebx, 0x359cef41	ff4518 88840decfeffff ff5638 69db41ef9c35	۳۱
cmp je mov sub cmp	ebx, 0xa1f6f5c8 0xfffffeca al, byte ptr [ebp + 0x7f] al, 0x41 al, 0x19	81fbc8f5f6a1 0f84c4feffff 8a457f 2c41 3c19	۳۲
cmp jne mov imul cmp	dword ptr [ebp + 0x6c], eax 0x1b eax, edi eax, ebx eax, 0x99788c79	39456c 7519 8bc7 0fafc3 3d798c7899 74cd 8b4560	۳۳

je mov	0xffffffcf eax, dword ptr [ebp + 0x60]		
call xor call and	dword ptr [esi + 0x14] edi, eax dword ptr [esi + 0x24] ebx, eax	ff5614 33f8 ff5624 23d8	۳۴
and or cmp jne sub call mov	ebx, 0x22bf9468 ebx, eax ebx, 0x5e29af15 0xb4 edi, 0x6ebec52 dword ptr [esi + 0x34] ebx, eax	81e36894bf22 0bd8 81fb15af295e 0f85ae000000 81ef52eceb06 ff5634 8bd8	۳۵
cmp jne call push	edi, 0x41056b6f 0x29b dword ptr [esi + 0x34] dword ptr [ebp + 0x18]	81ff6f6b0541 0f8595020000 ff5634 ff7518	۳۶

بدیهی است که بکارگیری این IoCهای استخراج شده نیازمند بازتعریف آن در قالب Rule هایی است که با توجه به نوع مکانیزم‌های دفاعی سازمان‌ها و فراهم کنندگان سرویس اینترنت، امکان درج در سامانه‌های IDS/IPS و UTM را داشته باشد. همچنین می‌توان سامانه سبک‌وزنی را تحت عنوان **تشخیص‌دهنده ترافیک مرتبط با باتنت Andromeda** طراحی و توسعه داد که با بکارگیری این رولها امکان شناسایی گره‌های آلوده شبکه (پشت NAT) را فراهم نماید که متعاقبا با بکارگیری آنتی ویروس مناسب قابل پاکسازی خواهند بود. انتظار می‌رود با طراحی و بکارگیری این محصول در سطح شبکه سازمانی و بکارگیری IOCهای مستخرج در GateWay سازمانی و شرکتی، نرخ آلوده‌سازی این بدافزار در سطح کشور کاهش چشم‌گیری پیدا کند.