تحلیل بات نت Stealrat و روشهای شناسایی و پاکسازی آن

مقدمه:

Stealratنوع جدیدی ازشبکه بات انتشار spam می باشد که از یک روش جدید برای انتشار spam استفاده می نماید و عملکرد این بات به شرح زیر می باشد:

- جمع آوری اطلاعات spam از قبیل نام فرستنده، نام گیرنده و فرمت ایمیل اسپم spamserver و ارسال آنها به سایت قربانی توسط سیستم آلوده به بات stealrat
- ارسال ایمیل های spam به کاربران توسط سایت قربانی
- ترغیب کاربران به کلیک بر روی لینک های ایمیل spam جهت هدایت به وب سایت قربانی دوم

در این مورد انتشار بدافزار توسط ایمیل spam انجام نمی گیرد بنابراین ارتباط میان ایمیل spam و بدافزار قابل مشاهده نیست. این ایمیل ها شامل لینک هایی است که کاربران را به وب سایت قربانی دوم هدایت می کند. در وب سایت دوم نیز لینک هایی وجود دارد که شامل صفحه وب آنلاین فروش دارو و یا صفحاتی است که کاربر را به کلیک بر روی آنها ترغیب می نماید.

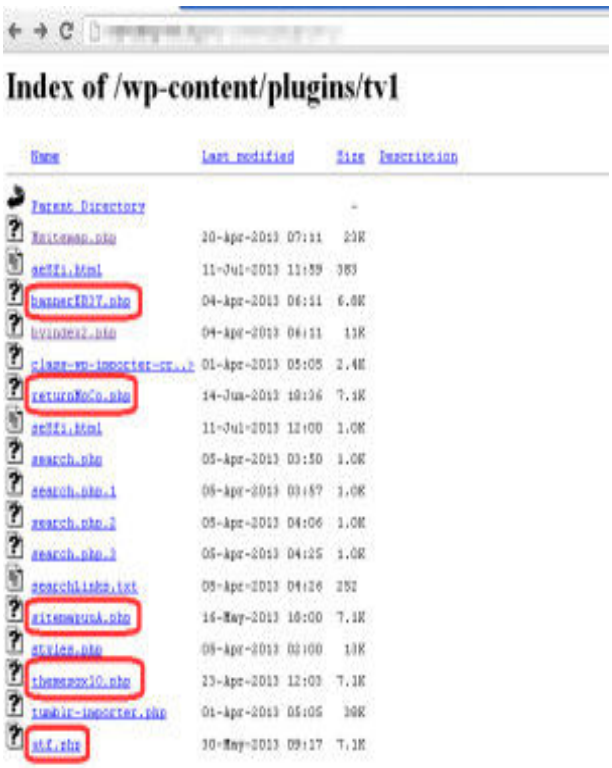
نکته جالب توجه این است که stealRat از طریق تغییر نام دامنه خود به google.com و پنهان سازی ترافیک شبکه و همچنین عدم ارتباط مستقیم با C&C سرور تلاش می نماید که ردپایی از خود بر جای نگذارد و تشخیص و شناسایی آن به آسانی انجام نگیرد.

بررسی وجود آلودگی

نقطه مشترک میان این وب سایت های آلوده اجرای نرم افزارهای آسیب پذیر CMS مانند وردپرس، جوملا و دروپال روی آنها می باشد. در ذیل مواردی را مشاهده می کنید که مدیران وب سایت می توانند آلودگی وب سایت را بررسی کرده و تشخیص دهند که آیا وب سایت قسمتی از بات نت stealrat می باشد یا نه:

۱.اولین قدم چک کردن اسکریپت های اسپمر است که عموماً با نام sm13e.php یا sm14e.php یافت می شود. اما توجه کنید که این اسکریپ ها ممکن است بر اساس نام فایل تغییر کند، لذا بهتر است هر فایل PHP ناآشنایی چک شود. نام فایل‌هایی که تاکنون شناسایی شده‌اند به شرح ذیل می‌باشد:

- copy.php
- up.php
- Del.php
- path.php
- bak.php
- utf.php
- bannerEB3Y.php
- returnMoCo.php
- sitemapuuA.php
- themesqx10.php



اسکریپ های اسپم در یک سایت آلوده

۲. راه دیگر شناسایی وجود فایل PHP آلوده، جستجوی هرکدام از رشته های زیر در کدها است:

```
(die(PHP_OS.chr(49).chr(48).chr(43).md5(0987654321
(die(PHP_OS.chr(49).chr(49).chr(43).md5(0987654321
```

در سیستم های لینوکسی می توانید رشته های ذکر شده را با دستور زیر جستجو نمایید:

```
/grep “die(PHP_OS.chr(49).chr(48).chr(43).md5(0987654321″ /path/to/www/folder
```

ولی در سیسنم های ویندوزی از دستور ذیل استفاده می شود:

```
scontent:”die(PHP_OS.chr(49).chr(48).chr(43).md5(0987654321″
```

رشته های ذکر شده در فایل PHP

این رشته ها قسمتی از کد “die” فایل PHP هستند (مثلاً وقتی که پارامتر خاصی را ندارد). تا آنجایی که می دانیم، آخرین نسخه از رشته موجود و در مقایسه با sm13e.php، فایل sm14e.php در حال حاضرچندین آدرس ایمیل را برای ارسال اسپم پشتیبانی می کند. علاوه بر آن فایل PHP یکسان که پارامترهای ذیل را قبول می کند، وجود دارد:

- l → email address (to send spam to)
- e → nine randomly generated characters
- m → mail server (ie. googlemail)
- d → mail template

پاسخ ها هم بسته به درخواست های ارسال شده و نیز روتین اسپم می تواند متغیر باشد .

	Code	Description	Example
Successful	chr(79).chr(75).md5(1234567890)+"0"	Spam is sent via the mail server specified in the POST data	OKe807f1fcf82d132f9bb018ca6738a19f+0
	chr(79).chr(75).md5(1234567890)+"1"	Spam is sent via the compromised website's SMTP server	OKe807f1fcf82d132f9bb018ca6738a19f+1
Unsuccessful	PHP_OS.chr(49).chr(48).chr(43).md5(0987654321)	Parameters in the POST data is less than 2	WINNT10+6fb42da0e32e07b61c9f0251fe627a9c LINUX10+6fb42da0e32e07b61c9f0251fe627a9c
	PHP_OS.chr(49).chr(49).chr(43).md5(0987654321)	There is no email address or email template in the POST data	WINNT11+6fb42da0e32e07b61c9f0251fe627a9c LINUX11+6fb42da0e32e07b61c9f0251fe627a9c
	PHP_OS.chr(50).chr(48).'+'.md5(0987654321)+[return value]	Failed to send spam via the compromised website's SMTP server	WINNT20+6fb42da0e32e07b61c9f0251fe627a9c+1 LINUX20+6fb42da0e32e07b61c9f0251fe627a9c+1

پاسخ های اسکریپ بر اساس نتایج

سطح تهدید بدافزار

نتیجه بررسی فایل تحلیل شده با استفاده از سایت Virustotal.com در جدول ذیل ارایه شده است. همانطور که مشاهده می‌شود از بین ۵۳ موتور تشخیص بدافزار ۲۳ عدد این فایل را به عنوان بدافزار تشخیص داده‌اند.

Antivirus	Result	Update
AVG	PHP/Agent.4	۲۰۱۶۰۱۰۴
Avast	[PHP:Spammer-D [Trj	۲۰۱۶۰۱۰۴
Avira	PHP/SpamBot.c	۲۰۱۶۰۱۰۳
Bkav	CPR59BC.Webshell	۲۰۱۵۱۲۳۱
CAT-QuickHeal	PHP.Pordwress.A	۲۰۱۶۰۱۰۲
ClamAV	PHP.Trojan.Spambot	۲۰۱۶۰۱۰۳
Comodo	UnclassifiedMalware	۲۰۱۶۰۱۰۴
Cyren	Trojan.UETG-2	۲۰۱۶۰۱۰۱
DrWeb	PHP.Spambot.6	۲۰۱۶۰۱۰۴
ESET-NOD32	PHP/Agent.DO	۲۰۱۵۱۲۳۱
Fortinet	PHP/Agent.DO!tr	۲۰۱۶۰۱۰۴
GData	Script.Trojan.Agent.11IMJG	۲۰۱۶۰۱۰۴
Ikarus	Backdoor.PHP.Shell	۲۰۱۵۱۲۳۱
Kaspersky	Backdoor.PHP.SpamBot.c	۲۰۱۶۰۱۰۳
McAfee	PHP/BackDoor-FBRG.a	۲۰۱۶۰۱۰۴
McAfee-GW-Edition	PHP/BackDoor-FBRG.a	۲۰۱۶۰۱۰۴
Microsoft	Backdoor:PHP/Shell.N	۲۰۱۶۰۱۰۴

NANO-Antivirus	Trojan.Html.SpamBot.cwyfhl	۲۰۱۶۰۱۰۴
Sophos	Troj/PHP-K	۲۰۱۶۰۱۰۴
Symantec	Trojan.Rodecap	۲۰۱۶۰۱۰۴
Tencent	Php.Backdoor.Spambot.Dygt	۲۰۱۶۰۱۰۴
TrendMicro	PHP_BACKSHELL.AE	۲۰۱۶۰۱۰۴
TrendMicro-HouseCall	PHP_BACKSHELL.AE	۲۰۱۶۰۱۰۴

راهکارهای پیشنهادی:

برای پاکسازی سیستم ها پیشنهاد می گردد فایل هایی که در بالا ذکر شده یا فایل های مشابه آن حذف و سیستم های مدیریت محتوای CMS ها- بخصوص وردپرس، جوملا و دروپال- بروزرسانی گردد. در ضمن محدود سازی ترافیک ارسالی و دریافتی در فایروال، بررسی مرتب لاگ های سیستم های امنیتی و آگاه رسانی به کارکنان در خصوص بازنکردن ایمیل ها، فایل ها و لینک های مشکوک به عدم آلوده شدن سیستم ها در آینده کمک بزرگی خواهد کرد.

خلاصه نحوه عملکرد و شناسایی بدافزار

در جدول زیر مشخصات بدافزار مذکور به همراه رویکرد تشخیص و پاکسازی به صورت خلاصه مشاهده می‌شود.

StealRat	نام	شناسنامه بدافزار
۲۰۱۰	سال کشف	
فایل های آلوده شبکه های اشتراک گذاری، پست های الکترونیکی هرزنامه، دستگاه های ذخیره سازی ثانویه مخرب و مراجعه به وب سایت های غیرمجاز	روش انتشار	
- ارسال هرزنامه - تزریق اسکریپت های مخرب PHP و HTML - غیرفعال کردن Task Manager، ابزار Registry و تنظیمات پوشه ها	تاثیرات	

✓ ارتباط با آدرس ها و IP زیر ✓ lyrics-db.org ✓ games-olympic.org ✓ mx1.games-olympic.org ✓ mx2.games-olympic.org ✓ newsleter.org ✓ t.newsleter.org ✓ bt.newsleter.org ✓ seek.newsleter.org ✓ fw.newsleter.org ✓ ۹۵,۱۶۳,۱۰۴,۶۸ ✓ ۹۵,۱۶۳,۱۰۴,۹۳ ✓ ۲۰۸,۱۱۵,۱۰۹,۵۳ ✓ ۸۵,۱۴۳,۱۶۶,۲۲۱	سطح شبکه	راهکارهای تشخیص
✓ اضافه شدن فایلهای زیر در سیستم ✓ • Application Data%\Microsoft\clipsrv.exe٪ • Application Data%\Microsoft\logman.exe٪ • Windows%\dllhost.exe٪ • Windows%\wininit.exe٪ • Windows%\System\ieudinit.exe٪ • System%\drivers\esentutl.exe٪ ✓ • System%\drivers\mstinit.exe٪ • System%\drivers\sessmgr.exe٪ • All Users%\dllhst3g.exe٪ ✓ ایجاد کلید رجیستری های زیر ✓ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\	سطح میزبان	

Explorer\Run "MqtgSVC = "%System%\mqtgsvc.exe /waitservice" ✓ HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Policies\ Explorer\Run "CmSTP = "%User Profile%\APPLIC~1\cmstp.exe /waitservice		

استفاده از آنتی ویروس های بروز یا ابزار SpyHunter	با استفاده از ابزار	راهکارهای پاکسازی
✓ استفاده از ابزارهای تحلیل ترافیک در میزبان و بررسی وجود یا عدم وجود ترافیک شبکه ای به آدرس IPهای ذکر شده ✓ نبودن اسکریپت های هرزنامه در پوشه های وب سایت ✓ نبودن فایل های ذکر شده در سیستم	بررسی پاک بودن سیستم	
✓ استفاده از ضد ویروس های تحت شبکه و بروز نگه داشتن آنها ✓ بلاک کردن HTTP User-Agent "Mozilla/5.0" و "-"در وب پراکسی ✓ بروزرسانی CMS در حال اجرا به آخرین نسخه موجود	سطح شبکه	راهکارهای پیشگیری
✓ به روز بودن نرم افزار ضدبدافزار نصب شده برروی سیستم ✓ اجتناب از دانلود و باز کردن فایل های ضمیمه پست الکترونیکی های ناشناس و نامعتبر	سطح میزبان	